8-2016

Gap analysis identifying the current state of information security within organizations working with victims of violence

Kelley K. Misata
Purdue University

Graduate School Form
30 Updated 12/26/2015

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Kelley K. Misata

Entitled
GAP ANALYSIS - IDENTIFYING THE CURRENT STATE OF INFORMATION SECURITY WITHIN ORGANIZATIONS WORKING WITH VICTIMS OF VIOLENCE

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Dr. Eugene H. Spafford
Co-chair

Dr. Marcus K. Rogers
Co-chair

Dr. Sorin A. Matei

Dr. Kathryn C. Seigfried-Spellar

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Dr. Eugene H. Spafford

Approved by: Dr. Eugene H. Spafford June 24, 2016

Head of the Departmental Graduate Program Date

GAP ANALYSIS IDENTIFYING THE CURRENT STATE OF INFORMATION SECURITY WITHIN ORGANIZATIONS WORKING WITH VICTIMS OF VIOLENCE

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Kelley K. Misata

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

August 2016

Purdue University

West Lafayette, Indiana

To my committee chairs, Dr. Eugene Spafford and Dr. Marcus Rogers, who put this amazing path in front of me – you saved me.

To my daughters, Amanda and Emily, who have endured stress cleaning, take-out dinners, and countless trips to Purdue – I love you!

To my best friend, Ray, who has held my hand throughout this journey -- your encouragement in my darkest moments has made this all possible.

To my Mom for your faith in me always.

ACKNOWLEDGEMENTS

First, I would like to express my sincere gratitude to Dr. Sorin Matei. Your support, encouragement, and amazing advice over the past four years has been invaluable. Our conversations and your ability to guide me with clear vision made all the difference in this process. Thank you for asking the hard questions, for pushing me further than I thought I could go, and for all your comments and encouragement.

Thank you also to Dr. Kate Seigfried-Spellar, for joining my committee late in the process and believing in the vision for this research.

I would also like to thank my friends in Brookline, MA – BillD, Elizabeth, Isabel, and Laura – who have been on this journey with me since the beginning. They have brought me coffee, fed me dinner when I forgot to get groceries, and allowed me to lean on them when the stress, pressure, and self-doubt manifested into tears. I will forever love you and be grateful for your support throughout this process.

Last, I would like to thank the Open Information Security Foundation team – Victor, Peter, Eric, Jason, Matt, and Andreas – for all your support and promises of chocolate. I am blessed to have such amazing colleagues.

TABLE OF CONTENTS

Page

Page

Page

Page

Page

LIST OF TABLES

Table Page

LIST OF FIGURES

Figure Page

ABSTRACT

Misata, Kelley K, Ph.D., Purdue University, August 2016. Gap Analysis Identifying the Current State of Information Security within Organizations Working with Victims of Violence. Major Professor: Dr. Eugene H. Spafford.

Around the world, domestic violence, human trafficking, and stalking affect millions of lives every day. According to a report published by the Center for Disease Control and Prevention in January 2015, every minute 20 people fall victim to physical violence perpetrated by an intimate partner in the United States (US). As offenders use advancements in technology to perpetuate abuse and isolate victims, the scale of services provided by crisis organizations must rise to meet the demand while keeping a close eye on potential digital security vulnerabilities. It has been reported in general media and research that phishing emails, social engineering attacks, denial of service attacks, and other data breaches are gaining popularity and affecting business environments of all sizes and in any sector, including organizations dedicated to working with victims of violence.

To address this, an exploratory research study to identify the current state of information security within the US-based non-profit crisis organizations was conducted. This study identified the gaps between a theoretical maximum level of information security and the observed level of information security in organizations working with victims of violence inspired by a recognized and respected framework, National Institute of Standards and

Technology (NIST) Cybersecurity Framework. This research establishes the critical foundation for researchers, security professionals, technology companies, and crisis organizations to develop assessment tools, technology solutions, training curriculum, awareness programs, and other strategic initiatives specific to crisis organizations and other non-profit organizations to aid them in improving information security for themselves and the victims they serve.

CHAPTER 1. INTRODUCTION

1.1 Problem Statement

Around the world, domestic violence, human trafficking, and stalking affect millions of lives every day. According to a report published by the Center for Disease Control and Prevention in January 2015, every minute 20 people fall victim to physical violence perpetrated by an intimate partner in the US. As offenders use advancements in technology to perpetuate abuse and isolate victims, the scale of services provided by crisis organizations must rise to meet the demand while keeping a close eye on potential digital security vulnerabilities. For example, phishing emails, social engineering attacks, denial of service attacks, and other data breaches affect organizations in many domains. Though research has not revealed direct cyber attacks on crisis organizations, this does not suggest that they are not invulnerable or immune to such attacks. A 2009 study from the Federal Bureau of Investigation (FBI) and the Privacy Rights Clearinghouse stated that non-profit organizations are most vulnerable to information security breaches that lead to identity theft (Kolb & Abdullah, 2009, p. 103). The report went on to state that from January 2005 to June 2007 a total of 155,048,651 records containing confidential personal information were stolen from various websites, including non-profit organizations (Kolb & Abdullah, 2009, p. 103). In addition, many who work in human services organizations have the misconceptions that information security measures are

costly, time consuming, and require implementation by technology exports. Overwhelmed by the complexities, crisis organizations often ignore the potential risks.

Little is known about the online information practices of non-profit organizations and how well they comply with best practices in information security (Hoy & Phelps, 2009, p. 72). In addition, researchers and security experts who ignore the information security of organizations that work with victims of violence leave these organizations and the people that they serve vulnerable to intrusion and attack. Research exists addressing how powerful technologies are used as a tool against victims of violence. However, there is a lack of research that evaluates how the organizations serving this sample struggle to understand the risks and institute effective information security strategies.

The information security of organizations that work with victims of violence is at risk for intrusion and attack, which perpetuates the lack of understanding around security tools, processes, and policies. To address this gap, an exploratory research study to identify the current state of information security within US-based non-profit crisis organizations is needed. It is possible to identify the gaps between a theoretical maximum level of information security and the observed level of information security in any given organization. This study measured and explored the gaps by looking at absolute and relative levels of information security preparedness using best practices inspired by a recognized and respected framework. Exploration of the gaps also determined the likely factors that correlate with the level of security preparedness. To be specific, the exploration looked at the degree to which organization type, the level of funding, division of labor with respect to information security policy implementation, and the number of

security tools might be associated with security preparedness as measured by an index for information security preparedness.

By identifying the current state, this study established the necessary foundation for researchers, security experts, and crisis organizations to work together to develop assessment tools, processes, and strategies specific for their environment and necessary to improve information security. In addition, using a national standard as a guide facilitated the development of assessment tools specific for crisis organizations to use in managing ongoing information security risks, opportunities, and priorities. This study advances the current state of research by assessing the information security ecosystems of crisis organizations using a recognized standard, thereby setting a foundation for future research in information security for crisis organizations as well as other non-profit organizations. Future research is needed to continue this effort and to bring the results of this study from theory to adoption

1.2 Purpose of Study

Crisis organizations are chartered to protect victims of abuse, trauma, and violence. Technologies used by an organization's staff, victims, and other legitimate users bring with them the possibility of digital intrusion, eavesdropping, and attack. With growing advancements in technology, crisis organizations and those they serve are at risk both in online and physical environments. Staff and survivors often forget this risk (R. Mednick, personal communication, August 2015). The collection, transfer, and storage of sensitive information in a digital format add additional risk management complexities for these organizations. Providing crisis organizations with viable strategies to improve their current state of information security first requires an exploratory review of the

information security paradigms, protocols, and points of vulnerability within these environments by using a gap analysis approach. As a result, the problem this research addresses is the identification of the current state of information security within crisis organizations through the examination of the gaps between absolute and relative levels of information security preparedness measured against best practices in a recognized cybersecurity framework. As stated previous, this research establishes a long overdue foundation for future research in the area of information security within crisis organization as well as other non-profit organizations.

Research in the domain of organizations working with victims of violence has focused on the use of technology by abusers and victims, stopping short of addressing the information security needs of the organizations missioned to offer resources and support to these victims. One example in which the use of technology by crisis organizations was questionable is in the 2012 survey conducted by the National Network to End Domestic Violence (NNEDV), which evaluated the use of technology by domestic violence agencies as a part of victim services (NNEDV, 2012). Results included responses from 378 out of 700 US domestic violence agencies covering a range of topics regarding technology used by staff, survivors, and abusers. Another study reporting on the utilization of the Internet and wireless communication by two Midwestern domestic violence shelters was conducted in 2002 (Kranz, 2002). This study involved a series of interviews with Executive Directors and staff comparing the use of the Internet and wireless communication in the service of domestic violence in urban and rural environments (Kranz, 2002).

In summary, the focus of existing research on how victims and abusers use technology has resulted in an oversight by researchers and security experts in addressing the challenges facing the organizations supporting victims of violence. Crisis organizations face many of the same challenges regarding information security as other businesses; however, the people they serve and the work they do creates unique complexities. To understand these complexities requires a different focus paired with academic rigor. In addition, by empowering crisis organizations with knowledge and confidence in the complicated arena of information security has possibility to improve the information security of the victims these organizations serve. As a result, the purpose of this study was to provide a needed foundation for future research so that information security within crisis organizations is no longer ignored

1.3 Research Question

As stated above, this research answers the question, what is the current state of information security within crisis organizations as measured against best practices in a recognized cybersecurity framework? The current state was identified by measuring the gaps in information security preparedness using best practices inspired by a recognized and respected framework. In addition, by conducting a gap analysis to address the above, researchers, security experts, and crisis organizations, the researcher established the necessary foundation to develop assessment tools, processes, and strategies to meet the specific needs and challenges facing crisis organizations. The results of this research made it possible to discover potential risks, opportunities for improvement, and priorities that crisis organization can use to improve the security of their digital environment and that of their victims.

1.4 Significance of the Study

The rise in the use of advanced information technologies and the adoption of the Internet into daily life has changed the way people gather information, communicate, and seek help. However, before the onslaught of smartphones, mobile applications, and social networking, crisis organizations used other non-technical methods to reach and protect the people they serve. Less than 20 years ago, domestic violence victims worked to keep their names out of telephone books, off post-boxes, and doorplates. They used aliases to pay bills. All of these protective measures were implemented to extricate themselves from victimization and to safeguard their locations (Zorza, 1995). For the organizations that support them, basic business functions, such as fundraising, community awareness, and operations management were restricted to the people and systems that had direct physical access to the organization and their communities. In today's technology-centric environment, new and creative approaches are required to protect crisis organizations and the victims they serve from intrusion and possible attack.

According to the National Center for Charitable Statistics, there were 1,076,309 non-profit 501(c)3 public charities reported in the United States in 2015 including hospitals, colleges, human services, museums, community foundations, and neighborhood organizations (National Center for Charitable Statistics, n.d.). In addition, 83,768 social welfare 501(c)4 non-profit organizations including civic associations, service clubs, advocacy organizations, and others were reported (National Center for Charitable Statistics, n.d.). As the number of victims continues to rise, so does the number of organizations and services needed to help them. As a result, a greater challenge in addressing the information security of this growing sample of organizations.

Research in the non-profit sector has suggested that information security deployment began in the 1960s, but seemed to lag behind for-profit organizations (Zhang, Gutierrez, Mathieson, & Wei, 2010). This early research identified some of the reasons for this lag, which are the result of a) limited budgets, b) lack of management support, c) insufficient training, and d) no technical support (Zhang, Gutierrez, Mathieson, & Wei, 2010). This research established the foundation to begin to identify whether non-profit crisis organizations have lagged even further behind their for-profit counterparts as technology has advanced, and if the reasons for the gap are the same.

Creating information security tools and protocols that are rife with complicated technologies and processes can be overwhelming for some non-technical users. In addition, for many users and organizations the belief is that security in a digital world is a state of all-or-nothing. Therefore, when addressing information security in any organizational environment it should be designed to serve the needs of the organization while keeping pace with changes in technology and threats (Needleman, 2001). For crisis organizations, information security strategies, tools, and processes should be designed to be relevant to securing their unique environment while not intruding on the activities to support and protect victims. The challenge is to help staff and clients use technology safely while still having all the benefits (L. Montanaro, personal communication, August 2015).

This study was the first to identify the information security for crisis organizations using a recognized framework. Using the gap analysis approach to assess the information security preparedness of crisis organizations was expected to generate a residual benefit. By raising the level of understanding and awareness by crisis organization staff provided,

as a result, new protective insights around information security that can be transferred with more confidence to victims, thereby improving their information security as well.

1.5 Operational Definitions

The following terms provide operational definitions for the purpose of this study. They are defined below for clarity and consistency throughout this study.

Crisis organizations are physical or virtual non-profit, non-government agencies, based in the United States, working with victims and survivors of domestic violence, physical and cyber stalking, sexual exploitation, and human trafficking. The direct or indirect services offered through these organizations may include medical, mental health, social work, and advocacy.

Information Security is a term that is often interchanged with "cyber security." For the purpose of this study and to ensure clarity for the reader, "information security" is used and defined as the practice of protecting information wherever it exists including cyber space.

Policies are internal policies related to use of technology, mobile devices, social media and other related operational policies concerning information security; also, governmental or policies outside the crisis organization may be referenced in relevance to this study.

Staff refers to employees (full and part-time), contractors, and volunteers working inside the crisis organization; does not include third party service providers or partners.

Victims is a term that is often interchanged with the term "survivor" throughout this study. Although a victim or survivor is often referred to in the feminine form, it is recognized that women, men, and children can be victims of violence.

Technology refers to computers, mobile devices, digital storage, communication via the Internet, privacy-protecting software, social media, and other security tools.

1.6 Research Objectives

The lack of existing research illustrates the need for an analysis of the current state information security within crisis organizations. To establish an achievable scope for this foundational research, this exploratory research study identified the gaps between a theoretical maximum level of information security and the observed level of information security within United States based non-profit crisis organizations.

Expanding the scope of this research to international crisis organizations can be addressed in future research initiatives. As stated above, this study measured and explored the gaps by examining the absolute and relative levels of information security preparedness using best practices inspired by a recognized and respected framework. The objectives of this study initiated that process by identifying the current state of information security within crisis organizations:

1. To document the gap between actual and ideal security policies and procedures within crisis organizations;
2. To document the gap between crisis organization who provide services to different categories of victims (e.g. domestic violence and human trafficking);
3. To document the gap across dimensions of security;
4. To examine if security preparedness is associated with information security solutions usage; and
5. To examine crisis organization characteristics (e.g. funding, lack of resources, lack of knowledge) associated with the gap.

The applied value of this research lies in establishing a necessary foundation for creating an accepted methodology that enables crisis organizations to raise awareness and improve information security within their organizations. As observed and discussed with crisis organizations during the National Network to End Domestic Violence Tech Summit (July 2015), the feeling of being lost in the complexities of technology makes it difficult for crisis organizations to help survivors safely navigate the growing technology domain.

1.7 Standards for Information Security

For this study, the baseline against which to measure crisis organizations against was established after a review of three recognized standards in information security:

1. International Organization for Standardization (ISO) ISO/IEC27001 – Information Security Management (ISO Management System Standards, n.d.);
2. Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT) 5 (ISACA, 2012); and
3. The NIST Cybersecurity Framework (CSF) (NIST, 2014).

Each is considered an industry leader and a benchmark for best practices in information security. Also, their messaging reinforces the importance of establishing and implementing information security systems, processes, protocols, and conversations that are grounded in the organization's needs, objectives, security requirements, size, and culture, all of which are consistent with the goals and objectives of this study. However, to stay within the scope of this research, one standard has been selected as the most

appropriate baseline for this study in respect to holistic view, simplicity in language and content, and availability.

1.7.1 International Organization for Standardization, ISO/IEC27001

In 1992, the Department of Trade and Industry (DTI) in the United Kingdom published a "Code of Practice for Information Security Management" (The History of ISO 17799 and ISO 27001, n.d.). Over the next 13 years, updates and new revisions of the International Organization for Standardization (ISO) family of standards were added. In 2005, the ISO 27001 was published, replacing BS7799-2 and designed for information security management systems aligning with ISO 17799 and compatible with ISO 9001 and ISO 14001 (The History of ISO 17799 and ISO 27001, n.d.). According to the ISO website, ISO/IEC 27001 is considered one of the most well-known standards in the ISO list of standards (ISO Management System Standards, n.d.).

The ISO/IEC 27001 provides the requirements for an information security management system (ISMS). Created through consensus by experts in information security, the ISO standard is considered a model to follow in "setting up and operating a management system" (ISO Management System Standards, n.d.). The following standards within the ISO family were reviewed in the context of the research objectives of this study (see Table 1 for ISO Management System Standards and Titles).

Table 1. *ISO Management System Standards*

ISO/IEC 27001	Information Management Systems
ISO/IEC 27002	Code of Practice for Information Security Controls
ISO/IEC 27004	Information Security Management – Measurement
ISO/IEC 270013	Guidance on the Integration implementation of ISO/IEC 27001 and ISO/IEC 2000-1
ISO/IEC 270014	Governance of Information Security
ISO/IEC 270015	Information Security Management Guidelines for Financial Services
ISO/IEC TR 27016	Information Security Management – Organizational Economics
ISO/IEC 27003	Information Management Systems – Implementation Guidance
ISO/IEC 27005	Information Security Risk Management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for Information Security Management Systems Auditing
ISO/IEC 27008	Guidelines for Auditors on Information Security Controls
ISO/IEC 27010	Information Security Management for Inter-Sector and Inter-Organizational Communications

Some of the components within ISO/IEC 27001 were in alignment with the objectives of this study. However, the other standards were outside the scope (ISO/IEC 2700, n.d.). Therefore, after review of the all the ISO standards above, it was determined by the author that the ISO suite is too complex in language and approach for this study.

1.7.2 Information Systems Audit and Control Association, COBIT 5

The Control Objectives for Information and Related Technology (COBIT) 5, an Information Systems Audit and Control Association (ISACA) framework for information security, is designed for the "governance and management of enterprise information technology" (ISACA, 2014, n/a). COBIT 5 is designed for technology professionals and business executives for use in any industry with organizations of any size (ISACA, 2012). It provides organizations with a systematic approach and common language to protect and manage information through five principles:

1. Meet stakeholder needs;
2. Cover the organization end to end;
3. Apply a single integrated framework;

4. Enable a holistic approach; and
5. Separate governance from management (ISACA, 2014).

COBIT 5 promotes itself as "generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector" (ISACA, 2014, n/a). However, the users of the framework are intended to be business executives and consultants in audit and assurance, compliance, IT operations, governance, and security and risk management. This is outside the scope of non-technical, often community-based crisis organizations. In consideration of the unique qualities of crisis organizations, COBIT 5 does recognize the importance that "information security is a business enabler that is strictly bound to stakeholder trust" (ISACA, 2014, n/a).

However, after reviewing the COBIT 5 system against the objectives of this study and through initial conversations with crisis organizations to help identify their current knowledge of information security and technology, it was determined that the framework is too complex in language and approach for inclusion. For future research and development of an assessment tool for crisis organizations, COBIT 5 should be considered.

1.7.3 National Institute of Standards and Technology Cybersecurity Framework

In February 2013, Executive Order 13636, Improving Critical Infrastructure Cybersecurity was the directive given to the NIST to develop a framework for critical infrastructures to reduce cyber risk (NIST, 2014). The NIST was charged with enlisting volunteer stakeholders in industry to provide input and validation to address the complete landscape of cyber security across business sectors. According to one of those stakeholders, the instructions were to design not a standard but a framework that was

transformative and built from the collective wisdom of thought-leaders in industry and government (T. Casey, personal conversation September 22, 2015). The goal of the NIST was to establish best practices and a framework that would foster security conversations at all levels within the organization. The NIST CSF was designed to provide a common language and to bridge the gaps between security and business (T. Casey, personal conversation September 22, 2015). "NIST's future framework role is reinforced by the Cybersecurity Enhancement Act of 2014 (Public Law 113-274), which calls on NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure" (NIST, 2015, para. 5).

In March 2016, Tenable Network Security reported the results from the Trends in Security Framework Adoption Survey (Cieslak, 2016). The survey involved over 200 information technology and security professionals in the US (Cieslak, 2016). The results reported that "84% of organizations across a wide range of sizes and industries already leverage some type of security framework" (Cieslak, 2016, para. 2). Though large non-profit organizations were included in the survey, it was not possible to determine if these included non-profit crisis organizations as well (R. Gula, personal conversation, April 5, 2016). However, results from this survey did report "larger organizations (5,000 employees or more) are more likely to adopt the NIST CSF (37%), 17% of smaller organizations surveyed (100 to 1,000 employees) also rely on this framework" (Cieslak, 2016, para. 6). Continued review of these survey results, including the barriers to adoption, may be useful for future research and development of an assessment tool, processes, and priorities for crisis organizations.

The NIST CSF consists of three primary components including the Framework Core, the Framework Profile, and Implementation Tiers. The CSF Core includes five functions—Identify, Protect, Detect, Respond, and Recover—that are intended to be viewed in a concurrent and continuous manner (NIST, 2014). Each function identifies categories and subcategories that map to existing standards, guidelines, and practices (see Appendix A). The Framework Profile "represents the cybersecurity outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories" (NIST, 2014, p. 5). Last, the Implementation Tiers exist to help "describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive)" (NIST, 2014, p. 5).

Each of the three components was reviewed, which resulted in the NIST CSF being chosen for this study. It was determined through the extensive review of all three frameworks reviewed for this study that the NIST CSF provided the best overall structure to support this and future research in this area. The NIST CSF is expected to be the most popular choice of security frameworks over the coming year (Dark Reading, 2016). In addition, to the cohesive alignment to the ISO/IEM 27001, COBIT5, and other standards not included in this review, the NIST CSF offers to best structure for this study and a viable starting point.

1.8 Assumptions and Limitations

The potential reputational and physical damage inflicted when an organization experiences a cyber attack can be devastating and have a permanent impact on the organization (Petel, 2004). Crisis organizations focusing on providing services to

survivors of trauma are not immune to this risk; however, they often lack the awareness, experience, and resources to assess their current vulnerabilities and respond to them. "Things are happening on our network or in our social media accounts, but we do not see it and would not know what to do if it happened anyway" (L. Montanaro, personal communication, August 2015). Crisis organizations are aware that cyber risks are all around, but they do not know what they are or how to address something if it does happen (R. Mednick, personal communication, August 2015). As a result, assumptions in this study included the following:

1. Crisis organizations lack the knowledge, policies, risk management, and business strategies regarding the use and risks of technology used by staff;
2. Crisis organizations are using technology, but have not identified the risk versus reward as it pertains to organizational strategies and information security; and
3. Crisis organizations have non-existent or limited policies and procedures regarding information security.

Potential limitations to this research existed in two areas. First, the predominance of research regarding survivor or abuser uses of technology helped to build the initial framework for this research, but overlooked the unique needs of the crisis organizations. Second, the level of technical understanding by crisis organization staff presented challenges in assessing the information security ecosystem in the data collection process. "Staff of agencies are social workers; they are not trained in information security or technology in general" (R. Mednick, personal communication, August 2015). As a result,

the development of the research methodology and survey for this study were designed with non-technical users in mind, in efforts to mitigate these limitations.

CHAPTER 2. LITERATURE REVIEW

As stated in Chapter 1, information security in crisis organizations has been overlooked by researchers and security experts. Extensive research across academic research, literature, and general media as conducted to establish a baseline of the crisis organization environment. This chapter summarizes this literature review and begins with a search for crisis organizations that work, direct and indirect, with victims of domestic violence, stalking, and human trafficking. Next, is an outline of information security in the non-profit sector and the opportunities for risk management strategies that can cross over in a relevant manner to crisis organizations. The chapter then addresses some of the vulnerabilities unique to crisis organizations as compared to other organizations in the non-profit and for-profit sectors

2.1 Technology

Advancements in technology have benefits for organizations working with victims of violence. With ease of technology, crisis organizations are now able to provide life-saving information, resources, support, counseling, and other services to victims through email, websites, social media, and electronic connections. “The spread of new media has also significantly increased non-profits ability to communicate with clients as well as regulators, volunteers, the media, and the general public” (Lovejoy & Saxton, 2012, p. 338). Also, many standard business operations for crisis organizations including

financial transactions, community outreach, and fundraising are now performed online. However, for these organizations to be effective, victims must feel safe accessing the website without the risk, for example, of leaving online traces for attackers and abusers to manipulate. Knowing where the vulnerabilities might exist initiates the process of identifying areas within the information security ecosystem that could be improved.

As in any business environment, even with a robust information security strategy in place, the impact of a cyber attack or breach can be devastating for the organization far beyond the event itself. "According to the World Economic Forum, a major critical information infrastructure breakdown may have a global cost of 250 billion dollars, and the probability of such an event ranges from 10% to 20%" (Armando, Costa, & Merlo, 2013, p. 253). However, a security strategy begins with understanding the business environment and the parts of the network—flow, data, access—that require protection. "The issue about controlling access to applications for particular users and searching for threats is a fundamental problem with which security teams often struggle" (Tokuyoshi, 2013, p. 13). For crisis organizations, like other businesses, an information security strategy must balance appropriate controls for the environment and the culture of the organization, without affecting accessibility and services for victims. To assess the information security needs and risks of crisis organizations, an assessment of their unique environments was conducted for this study. This effort reinforced the importance of knowing the organization's environment and the people working within the system before embarking on an information security assessment of the technology used by the organization.

2.2 Victims of Violence

Victims of violence span across many economic, demographic, geographic, and cultural domains. Crisis organizations, though missioned in one area, often offer services that meet the needs of victims across the spectrum. The scope of this study was narrowed to address the crisis and resource organizations specifically missioned to assist victims of domestic violence, stalking, and human trafficking in the US. Expanding the scope to include international victims of violence was noted for future research.

2.2.1 Domestic Violence and Stalking

According to a report published by the Center for Disease Control and Prevention in January 2015, every minute 20 people fall victim to physical violence perpetrated by an intimate partner in the US (Center for Disease Control and Prevention, 2015). Domestic violence is a "pattern of abusive behavior in any relationship that is used by one partner to gain or maintain power and control over another intimate partner" regardless of race, age, sexual orientation, gender, education level, or economic status (US Bureau of Justice: Domestic Violence Cases, n.d.). Though it often refers to violence between spouses (spousal abuse), it can include cohabitants and non-married intimate partners (US Bureau of Justice: Domestic Violence Cases, n.d.). Domestic violence spans across a spectrum that includes physical, sexual, emotional, economic, and psychological abuse through behaviors involving intimidation, manipulation, isolation, frightening, and humiliating (US Bureau of Justice: Domestic Violence Cases, n.d.). Similar, stalking is defined by the US Bureau of Justice as a "pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear" (US Bureau of Justice: Domestic Violence

Cases, n.d.). The domestic violence crisis organizations reviewed for during the preliminary research for this study indicated providing services for both domestic violence and stalking victims. These services include emergency shelter, housing, advocacy, referrals, court processes, children's programs, and community education. Understanding the scope of services provided initial points to investigate potential information security vulnerabilities.

Though, existing research did not address information security within crisis organizations there are a few examples of studies that address the use of technology by victims in crisis organizations. One such study was conducted by the National Public Radio (NPR). This study surveyed 70 domestic violence shelters to identify how prevalent technology is used to stalk and abuse survivors (Shahani, 2014). According to the study, some domestic violence shelters were conducting "digital detox" for victims when they first entered the shelter. Recommendations included shutting off GPS and WiFi and refraining from using Facebook (Shahani, 2014). In one survey, 85% of the shelters involved in a survey indicated they were working with victims whose abusers tracked them using GPS, and 75% of victims' report abusers eavesdropped using hidden mobile apps (Shahani, 2014). Several shelters in this report indicated they have a policy against using Facebook on premises because of the risk that an abuser could pinpoint the (physical) location of the organization (Shahani, 2014). This study, at minimum, provided some useful insights to begin to understand how crisis organizations address technology within their environments.

2.2.2 Human Trafficking

Many around the world recognize human trafficking as a form of slavery and an abomination of human rights. Human trafficking is an international enterprise of sexually exploitation people pornography, sex tourism, mail order brides, and forced prostitution (Corrigan, 2001). In 2001, researchers estimated that four million people are trafficked around the world every year as part of a global business that produces profits of up to $7 billion in US dollars each year (Corrigan, 2001). Researchers agreed that while trafficking patterns fluctuate with the global supply of and demand for trafficked victims, trafficking originates in impoverished areas that lack viable economic opportunities for victims (Corrigan, 2001). With advancing technologies, traffickers are now at a significant advantage in being able to communicate and access potential victims to expand their business operations; with the Internet, physical borders are often irrelevant (Corrigan, 2001). However, as with domestic violence and stalking crisis organizations, technology advancements aid crisis organizations in reaching victims and combatting traffickers. “Every year, the illegal traffic of women for the sex trade puts multitudes of women at risk of losing their personal freedom, suffering physical and emotional abuses, and being sexually exploited for the profit of others” (Corrigan, 2001, p. 16).

The human trafficking crisis organizations reviewed during the preliminary research for this study provided a variety of services to victims. Similar to domestic violence and stalking crisis organizations, organizations dedicated to assisting victims of human trafficking provide to victims’ assistance food, shelter, clothing, medical, legal, job training, and education. However, more than domestic violence and stalking crisis organizations, human trafficking organizations face additional challenges that are the

result of political, international, and cultural complexities—an important element to consider in future research.

2.3 The Non-Profit Sector

Researchers indicated that organizations in the non-profit sector are more at risk for an information security breach or attack because, in part, the volume and sensitivity of the data they capture and store on their systems (Biswas, 2015; Petel, 2004). For example, in a study conducted in 2014, "over a four-year period, Citizen Lab looked at more than 800 suspicious emails, and 2,800 malicious payloads and malware families used to target the organization" (Kirk, 2014, para. 5). The results of this study showed patterns that indicated the same China-based networks that attacked other government and industry targets also attacked some non-profit organizations. As reported, "two of the human rights groups, included one focused on Tibet, were struck by APT1, also known as the Comment Crew" (Kirk, 2014, para. 7). Also, Singapore's Personal Data Protection Commission (PDPC) held the third annual data protection conference, which included approximately 600 data protection officers from throughout the country of over 4 million citizens (Pfeifle, 2015). During the conference, PDPC's Leong Keng Thai was quoted regarding data breaches, "it is not only personal data that is lost, but also reputations of individuals and organizations are involved as well" (Pfeifle, 2015, para. 7).

Analysis of digital attacks against human rights groups showed that these organizations are being targeted for the same types of intrusions as large commercial organizations, but have far fewer resources to defend themselves (Kirk, 2004). Often non-profit organizations work on limited budgets with staff that may not possess the technical expertise and skills to best evaluate a given situation best (R. Mednick, personal

communication, June 2015). In addition, it may be a situation where attacks are less targeted or organizations are unaware they are even being attacked. Therefore, it is important to continue to emphasize that, though an attack has not been reported or realized, this does not mean it has taken place or will not occur. Crisis organizations are not immune information security attacks; in fact, they may be more at risk as a result of some of the vulnerabilities, which are outlined in the following section. As a result, it is critical that they begin to understand what is at risk, both digitally and physically.

2.4 Vulnerabilities for Crisis Organizations

Similar to other business environments, crisis organizations are receiving requests, answer questions, soliciting for donations, conducting business operations, and providing services to victims utilizing various forms of technology every day. Therefore, it has become necessary for staff within these organizations to become more aware of the technical, process, and behavioral risks that may alert an attack. In addition, they need to understand characteristics of malicious actors targeting crisis organizations. The following provides a brief analysis for the purpose of this study; however, further research to understand attacker personas is needed.

1. Abusers and traffickers are those controlling or abusing the victims;
2. Hackers are directed attackers interested in compromising the information security system through denial of service (DoS), advanced persistent threats, and other methods; and
3. Data mining attackers are those motivated by accessing aggregated user information or specific personal information on clients, donors or other stakeholders (Green, 2010).

These attackers, like non-malicious actors, are aware that crisis organizational websites provide a digital channel solicit information from victims, community members, other service providers, and donors; however, staff may be unaware of how their web use or browsing habits are being recorded.

> We were looking at our Google Analytics and can see someone from Bangladesh visiting our website with unusual frequency; we don't have a way to know if that is a problem or what to do about it if it was. (R. Mednick, personal communication, August 2015)

It is common knowledge among security experts and researchers that Internet service providers (ISP), hardware, software, how a website was accessed, which pages were viewed and for how long all put user information at risk for an attack in this organizations (Solve, 2011). Understanding the scope of what is being tracked through the organization's use of technology and online presence can help identify potential points of vulnerability for attack. The following subsections offer a sample of other points of vulnerability overlooked in the current crisis organization environment.

2.4.1 Data Breaches

As stated above, with advancements in technology being used perpetuate abuse and isolate victims, the scale of services provided by crisis organizations must to rise to meet the demand while keeping a close eye on potential data breaches. For example, phishing emails, social engineering attacks, denial of service attacks, and other data breaches affect businesses sectors both large and small. Though research has yet to reveal data security breaches specific to organizations working with victims of domestic violence, human trafficking, and stalking, it does not mean these organizations are immune to a data breach. Across the broader non-profit sector, researchers have

discovered cases of "non-profits who were either breached via a network compromise or even experienced physical theft of devices that gave perpetrators access to databases filled with valuable information such as names, addresses, and social security numbers" (Weedon, 2014, para. 6). Considering the services crisis organizations provide victims and the rise in media reports highlighting data breaches across business sectors, a data breach within this environment has the potential to put not just data, but lives, at risk.

> As we are learning after states began to pass laws requiring notification of data breaches and the subsequent blizzard of data breach reports, security of information in databases is often haphazard, a particular concern in the domestic violence context since a breach can impact the safety of potentially hundreds of victims. (Green, 2010, p. 280)

This study identified tools, processes, and protocols in which security safeguards were present to minimize the risk of a breach; these include automatic log-out systems, encryption, and an address-filtering firewall (Green, 2010). It also addressed tracking mechanisms for administrators to track access and provides an audit trail; even those credentials are at risk (Green, 2010). In addition, questions regarding the security of the transmission of the data, the storage of the database, and the protocols when data is purged from the organization were included in this study. For example, organizations using cloud-based information storage and sharing applications, such as Dropbox, revealed a key reason for using these technologies was the need for productivity-related applications to service victims and stakeholders. Consistent with other business environments, crisis organizations need to consider the productivity versus risk debate. This debate presents ongoing challenges for security experts and researchers as they work

to find safeguards for the usage of unmanaged, non-secure third party applications (Citrix, 2015).

2.4.2 Fundraising

Financial support for non-profit organizations comes a variety of sources. Crisis organizations are no different than other non-profit and human services organizations in having to exist on financial donations and the trust of the communities they serve. The organizations reviewed in the preliminary research for this study indicated on their websites that fundraising is key to survival (see Appendix B). In a study by Hoy and Phelps (2009) "online giving to the largest United States based non-government organizations (NGOs) grew from $880 million in 2005 to $1.2 billion in 2006" (p. 71). With the advancements in technology and payment processing, crisis organizations and other non-profits conduct fundraising activities both on and off line. The ease and reach to donors through online channels is attractive to many non-profit organizations. Crisis organizations may be putting themselves at risk without knowing it. For example, financial data is attractive to attackers motivated by identity theft, credit card theft, bank account information, and other personally identifiable details of a mass of donors or more targeted wealthy donors (Weedon, 2014). A simple website misconfiguration can expose an organization's database of donors and their personal information to a crisis.

Several of the organizations analyzed in the preliminary research for this study utilized online bank and payment processing companies such as PayPal, while others masked their payment methods, calling into question the level of security (see Appendix B). Several redirected visitors to the donation page on their website using HTTPS. Though HTTPS is one of the current web security protocols, it is rife with vulnerabilities,

a topic for future research. Visitors were then required to complete a fill-in form including personal identifiable and credit card information. None of the organizations in this preliminary study provided an option to donate anonymously nor did any of them state awareness around security, steps being taken to protect the identity of donors, or the transactions (see Appendix B).

Last, it is important for crisis organizations to consider that information security breaches that expose donor and staff details could open the organization to potential ligation should they be compromised. Non-profit organizations may not comprehend the risk of losses, direct and indirect, due to an information security failure until they face legal action. (Kolb & Abdullah, 2009). Such an event could cause a small crisis organization to go out of business.

2.4.3 Tracking Features

Organizations working with victims of domestic violence, stalking, and human trafficking are familiar with tracking techniques and risks in the physical domain. However, in a digital space, understanding the benefits and risks associated tracking features embedded in technology can be confusing for non-technical users. For example, cookies, in simple non-technical language, are small text files of code that are deployed on a computer when a web page is downloaded. When a victim or a donor visits a crisis organization website, an identifier is created in the cookie and stored on the user's hard drive. Web bugs, on the other hand, are hidden snippets of code that can gather data about the user, such as the destination of emails and websites being visited; some more malicious versions have the ability to access the target's computer files (Solove, 2004).

For non-malicious purposes, the organization can see where visitors spend their time and provides information about how improve the site. From the perspective of crisis organizations, this information can be useful in improving and refining the site. However, this tracking capability can be leveraged by attackers as they can track their victims within a crisis organization's website, social media, and other channels. Gaining greater understanding of these features, along with the risks and benefits to the organization, become key in the analysis of the current state of information security within crisis organizations.

Last, many crisis organization websites reviewed during the preliminary research for this study have "escape" buttons that allow users to click to another page (see Appendix B). However, in some instances cookies and images from all of their web surfing remain on victim's computers if other security measures are not taken. Navigating to a new website does not erase these and does not guarantee that an abuser would not later access the computer and view the victim's Internet history. Consider a scenario where an "escape" button on a crisis organization website is vulnerable in a manner that an attacker can disable or redirect the "escape" feature, thereby putting victims at risk. The examples outlined above are not intended to be exhaustive, but simply a baseline to begin as advancements in technology also introduce other devices and fingerprint technologies with better tracking features that should be considered for future research.

2.4.4 Mobile Devices

The influx of mobile devices used by staff, clients, and other stakeholders in business environments has raised numerous concerns from security experts and researchers. With the availability of interception and infiltration technologies on

smartphones and other advancing technologies, the entire business infrastructure is now at risk as a result of bring your own device (BYOD) practices. Crisis organizations also need to take these risks into consideration. Caller ID, call logs, text messaging capabilities, online billing, and mobile devices are all points of concern when evaluating an information security ecosystem (Cantwell, 2007). This is vital when evaluating the crisis organization environment where 24-hour-a-day access to victims and other service providers is essential. For many organizations, adopting comprehensive mobile security protocols and policies does not suggest banning the technology, but rather incorporating them with security in mind. According to the 2015 State of Endpoint Security whitepaper from the Poneman Institute, "The biggest problem identified in this year's research is the negligent or careless employee with multiple mobile devices using commercial cloud apps and working outside the office" (Poneman Institute, 2015, p. 2).

The Poneman Institute study goes on to reveal that 68% of 703 IT professionals surveyed indicate that employee-owned mobile devices, such as Android, iPhones, and Blackberry mobile phones, risk endpoint security (Poneman Institute, 2016). Figure 1 identifies the reasons for the rise in endpoint risk as reported by the Poneman Institute study in 2016.

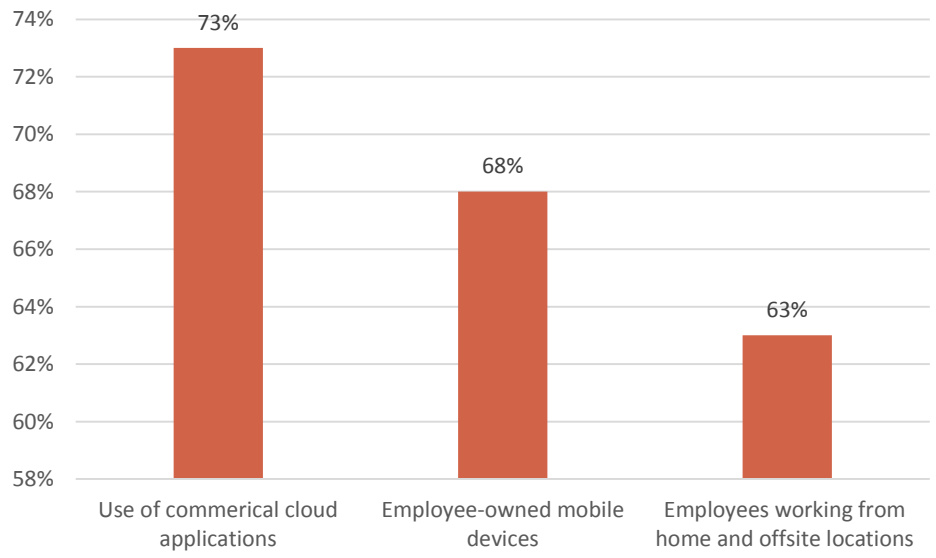


Figure 1. Reasons for Endpoint Risk Increase as Reported by the Poneman Institute, 2016.

Unique to crisis organizations, staff and advocates are discovering that abusers are getting savvy to technology and finding work-around solutions to track and control their victims. For example, domestic violence abusers might give their children smartphones installed with malicious and hidden tracking software to track their spouse (Shahani, 2014). By evaluating policies around BYOD, mobile and other endpoints security help crisis organization to identify other points of vulnerability over which they may or may not have control.

2.4.5 Endpoint Security

Endpoint security, including security for servers, desktops, laptops, smartphone, printers, ATMs, and "point of sale" (PoS) devices, must also not be overlooked when assessing the current state of information security within crisis organizations. Once again,

the 2015 study conducted by the Poneman Institute highlighted the importance of looking at endpoint security in any business environment (Poneman Institute, 2015). The results relevant for this study included:

1. Employees are the greatest source of endpoint risk;
2. Mobile endpoints are an increasing target of malware;
3. Endpoint security is becoming a priority;
4. Web-borne malware attacks are increasing in frequency;
5. Adobe (e.g. Acrobat, Flash Player, Reader) (62 percent of respondents), Oracle Java JRE (54 percent of respondents) and third-party cloud-based productivity apps (e.g. WinZip, VLC, Vmware and VNC) are all considered high risk;
6. Smartphones are the greatest risk to IT security; and
7. Governance and control process are the biggest gaps in preventing attacks (Poneman Institute, 2015).

2.4.6 Monitoring and Eavesdropping Software

There is an increasing number of monitoring software applications available for easy installation on computers, either remote or direct onto the device. Such applications have the ability to record all e-mails, chats, instant messaging, websites visited, keystrokes typed, and programs launched; they can also activate webcams and capture user passwords—all of which can transmit this information from a victim to the attacker's device with ease and a degree of anonymity (Cantwell, 2007). Research revealed that 75% of domestic violence organizations have indicated that they worked with victims whose abusers eavesdrop on their conversation through hidden mobile apps

(Shahani, 2014). As an example, Mspy is software that does location tracking, including a map within the application that shows where the victim or staff member's smartphone is and even the route it took to get from point A to point B (Shahani, 2014). Mspy also has an eavesdropping function that allows stalkers to listen in on incoming calls on their victims' phone.

> The target gets an incoming call, that very second, their speakerphone gets activated and starts recording. The victim doesn't have to answer the phone. The ringer could even be on mute, so you don't know it's ringing. But whatever conversation is happening in that room — say the victim is talking with her sister or her counselor — the smartphone feeds it back to the stalker. (Shahani, 2014, para. 28)

The growing availability and ease of use with monitoring and eavesdropping technologies have added to the open points of vulnerability for the crisis organizations and the victims they serve. These technologies have the ability to put into the hands of an abuser or trafficker safety plans, addresses, contact information, and other information—also putting crisis organization staff at risk.

2.4.7 Online Communities

Building communities online has become a valuable tool used in every business sector. It is not a surprise that crisis organizations and other human service agencies have seen the importance of building online communities and using social media for visibility, community education, information, referral services, online counseling, and advocacy activities (Finn & Banach, 2000). For these organizations, online communities and the social media platforms being used to facilitate them have become standard business practice. For victims, these online communities that connect them to resources, help, and others like them are also lifelines.

A 2012 study by Lovejoy and Saxton reported four categories in which the use of social media contributes to fostering community within non-profit sectors and are relevant in this study in crisis organizations:

1. Giving recognition and thanks;
2. Acknowledgement of current and local events;
3. Response to public rely messages; and
4. Response to solicitation. (p. 344 – 345)

Research has also shown that social media platforms used by crisis organizations have also provided useful for online assessments, outreach to victims, victim groups, victim art, and platforms for victim stories (Finn, 1996). “Our Facebook page is not where clients go; it is where we try and update the community in Cambridge of what we are doing and fundraising” (R. Mednick, personal communication, August 2015). As preliminary research for this study, a brief analysis of the social media platforms being used by a randomly selected group of 20 crisis organizations was conducted (see Appendix B).

Each website varied in design, informational detail, and support available to clients and other stakeholders online. The types of social media used also varied and warrant additional research into how it they used, who uses them and when, and what security measures (technical and policy) have been considered or instituted. However, none of the websites mentioned privacy policies or practices regarding the use of social media. Several also failed to mention privacy in regards to online donations as discussed in section 2.4.2 Fundraising.

There are positive attributes to building online communities, as indicated by researchers, including broader and direct outreach, community engagement, and survivors' services. However, all this comes with significant risks, including threats to personal safety, breaches of confidential information and conversations, compromises to privacy, and challenges to service delivery (Banach & Bernat, 2000; Finn, 2000; Waldron, Lavitt, & Kelley 2000). "Evidence from social networking sites may be the evidentiary basis that a victim has for obtaining a protection order" (Baughman, 2010, p. 946). Also, "fraud is a widespread issue that has emerged regarding social networking and is thus relevant when discussing the admission of social networking evidence" (Baughman, 2010, p. 953). As breaches and security flaws through these channels continue to mount, crisis organizations evaluate the risks versus the benefits. Do the benefits of social media outweigh the risks to privacy, data, and reputation? Many organizations suspect malicious activity is happening on their network and/or in social media accounts. However, they do not have the skills or tools to recognize it and would not know how to address it (L. Montanaro, personal communication August 2015).

2.4.8 Privacy

Privacy is the ability to control the circumstances in which personal, identifiable information is captured and used (Hoy & Phelps, 2009, p. 72). To support fundraising activities, community engagement, and victims' services, crisis organizations rely on the gathering of personal information from donors, volunteers, stakeholders, and victims in person and online. However, any organization that collects personal information direct or indirect has a responsibility to keep that information secure, which is a key area to understanding the current state of information security within crisis organizations.

"Although online consumer privacy has been an important issue for the commercial and regulatory realm, non-profits did not begin to address these issues until much later" (Hoy & Phelps, 2009, p. 72).

For victims of violence and the staff working with them, adding layers of trauma, stress, and urgency brings additional challenges to issues of privacy and services. Some crisis organizations may assume the information they are collecting would not appear to be attractive to malicious actors (Rezgui, Bouguettaya, & Eltoweissy, 2003). However, when looking at the risk through a wider lens, the information does present targets for attack. To illustrate this further, a brief analysis of the areas within the crisis organizations vulnerable to privacy intrusion was conducted. Though the headings compiled for this list came from a research study conducted by Eltoweissy, Rezgui, and Bouguettaya (2003), the analysis was customized for the objectives of this study and to address the unique characteristics of information security within crisis organizations.

Access Control is the act of identifying other points of access when the focus is on direct victim services may result in a vulnerability point not previously considered. For example, what if a malicious actor were to gain access to an organization's donor list, including names, addresses, emails, credit cards, and other details? The processing of donations and other business functions through their websites present a risk that can be enormous and fatal for some crisis organizations. The consequences are even more important when the attack target is a system containing sensitive information about groups of people. For example, "In 2000, a hacker penetrated a Seattle hospital's computer network, extracting files containing information on more than 5,000 patients" (Rezgui, Bouguettaya, & Eltoweissy, 2003, p. 4).

The Collection of Data occurs when crisis organizations are unaware of how and when their information is being collected. Harvesting user data and patterns; indirectly collecting information can paint both accurate and inaccurate portrayals of users (Rezgui, Bouguettaya, & Eltoweissy, 2003).

Information Brokers are individuals, attackers, or distributed information brokers who collect personal and identifying information. These brokers can obtain information, such as the current address of a victim. Information can be purchased in bulk, or requested by brokers using the "darknet." An abundance of information is available free on the Internet through courts and other organizations as a matter of public information (Cantwell, 2007).

2.4.9 Trust

For non-profits, in particular crisis organizations, trust "lies in the heart of charity" (Sargennt & Lee, 2002, pg. 68) Trust is essential; however, the privacy concerns and risks in relationship to information security have the potential to undermine trust (Hoy & Phelps, 2009, p. 72). In its 1998 report *Privacy Online: A Report to Congress*, the FTC described accepted fair information practice principles of Notice, Choice, Access, and Security (Federal Trade Commission, 2000, pg. *i*). Relevant for this study, under the Notice principal, the report stated:

> The Web sites would be required to provide consumers clear and conspicuous notice of their information practices, including what information they collect, how they collect it (e.g., directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access, and Security to consumers, whether they disclose the information collected to other entities, and whether other entities are collecting information through the site. (Federal Trade Commission, 2000, pg. *iii*)

Intrusions or breaches in physical security, information security, and privacy can have dramatic impact on the trust held across staff, volunteers, victims, and the community, thereby affecting services to victims. In addition, compromises in trust can influence donors to give and victim to use the services offered by organization (Hoy & Phelps, 2009, p. 80). A 2002 study reported that the reasons why donors stop giving to non-profit organizations is a "perceived lack of trustworthiness" (Hoy & Phelps, 2009, p. 80). As a result, situations, such as information security breaches and attacks, that comprise trust in crisis organizations can have direct impact to the organization to service victims, to raise funds, and stay in business. Therefore, the importance of trust cannot be minimized in any environment missioned to protect and save lives.

2.4.10 Other Risks

In recent years, the conversations around digital security, privacy, confidentiality, and the mass collection of information have increased. For this study, crisis organizations were asked to inventory the existing technologies they use. This list was formulated from the preliminary research for this study and the outline of risks detailed below:

1. Facsimile machines operate through telephone lines that can be compromised, often include sender details on the receiving transmission, and in some cases keep a log of sent and received faxes on the device; all create points of data breach vulnerabilities.
2. Teletypewriters (TTYs) provide assistance to clients and others with hearing impairments by providing text-based phones. If used by a crisis organization, it is important to consider how the content and logs of those conversations are

being stored. In some cases, attackers can use this technology to impersonate a victim (Cantwell, 2007).

3. Global Positioning Systems (GPS) make it easy for an attacker to monitor location(s) of their victim(s) as well as staff. “Counselors in St. Paul, MN had to call the police when an abuser banged on the safe house doors; he had tracked down his wife using GPS” (Shahani, 2014, para. 12).
4. Webcams are a standard built-in feature on many phones, laptops, and desktop devices. However, it is easy for abusers to turn on these cameras from remote locations. Often undetected, the give the abuser the capability of conducting video surveillance targeting their victim.
5. The Internet of Things (IoT) is the “networked interconnection of everyday objects, which are often equipped with ubiquitous intelligence” (Xia, Yang, Wang, & Vinel, 2012, pg. 1101). Conversations concerning the benefits and risks of IoT are just beginning in the security community. However, the flux of technologies across all aspects of life “leads to a highly distributed network of devices communicating with human beings as well as other devices” (Xia, Yang, Wang, & Vinel, 2012, pg. 1101). These connections need to be taken into consideration for information security within crisis organizations.

2.5 Opportunities for Improvement

Researchers, security experts, and technology companies offer users numerous tips, checklists, and suggestions to improve their security online. A consistent and significant theme throughout is the importance of increasing awareness, training, and ongoing education to improve information security within any business environment. For

the purpose of this study and summarized from preliminary research in this area, the following were determined as baseline theories and methods appropriate for crisis organizations to improve information security:

1. Dispel the myth that security is 100% effective 100% of the time;
2. Direct staff, victims, and stakeholders on how to evaluate at their individual security, including protecting personal information, email, deleting traces of web access, personal firewalls, remailers, trace removers, encryption, and anonymizers (Rezgui, Bouguettaya & Eltoweissy, 2003);
3. Investigate network security solutions including VPNS, firewalls, IDS/IPS technologies;
4. Understand motives for attacks. Even though the reasons may not be obvious, some crisis organizations can be targeted for attack because of information that is attractive in a commercial market, thereby breaking a trust network in the community, or for their contact database (Leach, 2014);
5. Keep pace with technology. Determining whether the computer systems (hardware and software) are up-to-date is a point of future research;
6. Assume an attack will happen. Organizations or individuals cannot prepare for every possible scenario lurking in a malicious attacker's mind, so keeping abreast of trends and risks is part of the challenge;
7. Invest in protection that is reasonable for the risks. Crisis organizations may overlook the fact that, like other NGOs, they exist because of financial contributions and donations from individuals and institutions. As mentioned

previous, this makes the organizations and their donors easy targets for malicious actors (Leach, 2014);

8. Build ongoing awareness and education and training programs for staff, survivors, and stakeholders who interact with the crisis organizations;
9. Identify and work to remove the weak links in the security landscape;
10. Educate staff and victims on different technologies, their use, the potential risks, and how to be safe. For example, personal devices are anything that connects to the Internet, including servers, tablets, cellphones, computers, printers, copiers, and fax machines. Opportunities for future research include educating non-technical users within crisis organization on remote management features, anti-virus solutions, browser and application protections, lock and erase functions, password management, device and software maintenance, and procedures to follow when anomalies are detected;
11. Connect. Connection refers to how, when, and where a device connects online which will determine the level of protection needed and what could be at risk. One aspect of research is determining if the organization is knowledgeable as to the risks and rewards of using VPNs and other privacy-protecting technologies;
12. Identify vulnerabilities. Email has become a standard in communications and often a certain point of vulnerability either from a possible data breach or a violation of privacy policies. For example, using a service that automatically

strips IP location and metadata information could provide protection to the crisis organization and the people they serve (Deflin, 2015); and

13. Implement the use of electronic documents, which require a digital vault to keep critical information safe from eavesdroppers or malicious hackers.

2.6 Summary

Like other businesses, crisis organizations are not safe from current or future information security attacks or breaches. However, since many attacks have not been detected or reported, it is safe to assume that it is only a matter of time. Research in other business sectors and the broader view of non-profits has documented the activities of malicious attackers to disrupt websites, intercept emails, spam, send malware/viruses, harass people, create false messages for help, and impersonate individuals. (McGregor, 2014; Peterson, 2015) "Data about more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data since 2009" (Peterson, 2015, para. 2).

This initial review of the crisis organization environment addressed a few vulnerabilities to illustrate the complexities and challenges they face. However, other challenges exist for both non-profit and crisis organizations that "struggle to acquire and maintain information and communication technologies because of high prices for the products themselves and the costs of training personnel" (Technology & Human Trafficking, 2011, para. 24). As the results of this study are examined in the following chapters and future research in this area commences, it will become evident that identifying the current state of information security benefits both the crisis organizations and the victims they serve by providing them with increased awareness, experience, and

knowledge with security technologies, policies, and behaviors that improve physical and online safety. For example, by not understanding the risks associated with using HTTPS web content or by clicking "TRUST" when a certificate authority cannot be validated puts staff and users at risk for eavesdropping and tracking.

The analysis of crisis organization environment, within the scope of this study, has begun. However, continued research is needed to better understand the unique characteristics of these organizations in regards to information security and advancing technologies.

CHAPTER 3. CONCEPTUAL MODEL

This chapter outlines the conceptual model for this study to address the gaps between actual and ideal states of information security preparedness within crisis organizations. In addition to the preliminary research, literature, and general media review conducted, this initial analysis includes excerpts from in-person communication with the following:

1. Risa Mednick, Executive Director of Transition House Domestic Violence Shelter;
2. Lauren Montanaro, Residential Advocate for REACH Beyond Domestic Violence;
3. Kaofeng Lee, Deputy Director of the Safety Net Project and the National Network to End Domestic Violence;
4. Leah Treitman, Program Coordinator at Thorn;
5. Delaney Workman, Demand Abolition Social Innovation Coordinator at Hunter Alternatives; and
6. Dhakir Warren, Senior Manager, Social Innovation at Hunter Alternatives in Cambridge, Massachusetts.

Their direct knowledge of crisis organizations and the challenges faced due to advancements in technology provided useful insights to the approach for this study and continued research and development of tools, processes, and strategies in this area.

3.1 Crisis Organizations Defined

With the minimal amount of research available on the information security ecosystem of crisis organizations, a preliminary research of two crisis organizations in the Boston, MA area was conducted. First, Transition House, a 501(3) non-profit domestic violence shelter and resource center has been serving survivors in Cambridge, MA since 1997 (Transition House, n.d.). The organization offers "a full circle of housing and holistic support for adults and children overcoming the trauma of family and partner violence" (Transition House, n.d.). As with other crisis organizations, Transition House provides safety planning, community education, and youth peer mentoring on healthy relationship development to help prevent the cycles of abuse (Transition House, n.d.). Conversations in preparation for this study were conducted with Risa Mednick, Executive Director of Transition House in March 2015, June 2015, and August 2015. According to Mednick, Transition House is facing two predominant challenges regarding information security:

1. "When working with victims of violence and crisis, we are working in the present psychological trauma. Teasing out how technology is playing a role is even more difficult."
2. "We are equally at risk as the people we serve when they enter our space physically and online. I think that is often forgotten in a digital space" (R. Mednick, personal communication, June 2015).

The second organization included in this study was REACH Beyond Domestic Violence, serving 27 communities in the Boston, MA area. REACH's mission is to "advance the safety, healing and empowerment of those who experience domestic or

relationship violence through direct services and education while promoting social justice for individuals and families of all backgrounds" (Reach Ma | Building Healthy Communities by Ending Domestic Violence, n.d.). REACH's executive director, Laura Van Zandt, provided an introduction to Lauren Montanaro, Residential Advocate as the point of contact for these initial conversations in June and August 2015. REACH's top priority is having access to safe, affordable housing for survivors, then focusing on help survivors manage finances including disability checks, job searches, and child care (L. Montanaro, personal communication, June 2015).

Continuing, Montanaro identified several challenges to helping organizations understand information security. For example, "getting people (within and outside the organization) to take the issue of cyber security seriously; survivors and staff often dismiss the risk they bring to the shelter through their devices" (L. Montanaro, personal communication, June 2015). Second, "staff does not feel confident to talk about technology and security, so they do not," leaving the organization, the staff and the survivors at risk (L. Montanaro, personal communication, June 2015).

In addition, initial discussions with representatives from Thorn and Demand Abolition confirmed that organizations working with victims of human trafficking and sexual exploitation share the viewpoints expressed above. Follow-up conversations with all of these organizations will continue through this study and as research and development continues.

3.2 Opportunities

As discussed in Chapter 1, recognized standards and frameworks to assist in assessing and improving information security within businesses of all sizes and in various

sectors are available. By using a recognized and respected framework not only provides organizations with a roadmap to follow, but also common language to use in follow-up conversations with researchers and security professionals. However, navigating through the technical language and complexities of these recognized standards and frameworks may prove to be overwhelming for crisis organizations challenged with limited staff, minimal budgets, and inadequate knowledge of information security terminology and systems.

The number of possible outcomes when using a robust framework can be enormous and span a wide array of areas of opportunity. However, in alignment with the objectives and scope of this study in identified the gaps of information security preparedness within crisis organizations, three key opportunities for using the NIST CSF have been identified. First, to establish the ideal state of information security as the baseline for the gap analysis begins with building trust and confidence. Using the terminology and flow of the framework for this and ongoing research initiated that process with crisis organizations while increasing their familiarity of what is needed to be secure (NIST, 2014). Second, by using the NIST framework, the risks, opportunities, and priorities for improving their current state of information security were identified through the gap analysis. Last, this gap analysis process identified the core baseline of an information security assessment tool for crisis organizations to use with efficiency and success.

Researchers from Alien Vault offer a useful list of 10 tips to help non-profit organizations. However, the research failed to provide this information through the lens of non-profits working with victims of violence (Biswas, 2015). Also, Confidentiality and

Sexual Violence Survivors: A Toolkit for State Coalitions (2005) offered additional useful questions for crisis organizations to consider. This study and future research examined these and other "checklists" to determine which ones best suited the environment of crisis organizations. As an example, the following list was adapted from current research and was incorporated into the data collection for this study:

1. Have a plan;
2. Decide what information is critical;
3. Design backup systems;
4. Create education and training programs;
5. Stay current with technology, threats, and behaviors so that policies and systems can keep step;
6. Invest in security technologies such as firewalls, encryption solutions, VPNs, etc.
7. Restrict access to help reduce risk that may be inherent in someone not remaining aware; and
8. Secure the entire environment including wireless networks, BYOD policies, and ways to monitoring staff security behaviors (Biswas, 2015) (Confidentiality and Sexual Violence Survivors, 2005).

3.3 Research Focus and Gap Analysis

In the 2012 NNEDV survey, crisis organizations identified their top concerns regarding the use of technology in their agencies. The results included:

1. Survivor use of social media and Skype thereby compromising security, location, and safety of the organization;

2. Survivor sharing identifying details on Facebook and other social media platforms;
3. Survivor making public statements online that could have a negative effect on the organization;
4. Staff setting appropriate boundaries when using social media;
5. Mobile devices use in the shelter with GPS locators; and
6. Residents using mobile devices at the shelters (NNEDV, 2012).

However, what was lacking in this survey was a holistic view of the state of information security within domestic violence, stalking, and human trafficking crisis organizations. As a result, the focus of this study was to analyze the gaps between absolute and relative levels of information security preparedness using best practices inspired by a recognized and respected framework. Through this focused effort and exploration of the gaps, this study reported on potential factors that correlated to information security preparedness such as organization type, the level of funding, division of labor with respect to information security policy implementation, and the number of security tools used within the organization. In addition, due to the lack of research with regards to information security within crisis organizations, this study also identified the characteristics of crisis organizations (e.g. funding, lack of resources, lack of knowledge) associated with the gap.

3.4 Summary

Research has shown the emphasis and importance of victims' use of technology and the complexities involving technologies, policies, and human behavior. Research also demonstrated a minimal focus on the unique characteristics of organizations working

with victims of violence. This research has the potential to provide benefits to society by identifying the risks, opportunities, and priorities crisis organizations can address to improve their current state of information security as measured against a recognized standard. As crisis organizations develop the ability to defend against attacks, an added potential benefit is increasing knowledge of information security and awareness among the victims they work with every day.

Researchers and security experts have overlooked crisis organizations working with victims of domestic violence, human trafficking, and stalking. With the growing threat landscape across all industries, the rise in victims of violence around the world and the prevalence of technology in society, the need to conduct research at the organizational level is urgent. As observed by the author at the 2015 NNEDV Technology Summit, crisis organizations are making some efforts to understand technology, policies, laws, and behaviors that are putting survivors at risk in a digital domain. However, this research took are more comprehensive view by identifying the current state of information security within crisis organizations to identify risks, opportunities for improvement, and priorities providing them with next steps for action.

CHAPTER 4. METHODOLOGY

Current research has revealed an emphasis on victim use of technology, with minimal focus on the information security in crisis organizations. The urgency for this research is evident in conversations with domestic violence organizations attending the National Network to End Domestic Violence (July 2015) and personal conversations with representatives from Transition House, NNEDV, Thorn, REACH Beyond Domestic Violence, and Demand Abolition (K. Lee, personal communication, September 2015; R. Mednick, personal communication, August 2015; L. Montanaro, personal communication, August 2015; L. Treitman, personal communication, September 2015; D. Workman & D. Warren, personal communication, October 2015). As a result, this chapter provides a description of the research design, procedures, and analysis conducted for this study. The methodologies chosen for this study support the research goal to identify the gaps between a theoretical maximum level of information security and the observed level of information security in any given organization, as well as, audiences for which the results of this study could impact. It explored the gaps by examining the absolute and relative levels of information security preparedness using three functions of the NIST CSF, which are Identify, Protect, and Respond (NIST, 2014). The methodology also allowed for characteristics of crisis organizations under the context of information security to be documented for this and future research.

4.1 Research Protocol

This study identified the current state of information security of a subset of crisis organizations by observing and reporting their actual versus ideal state of information security preparedness using the NIST CSF (NIST, 2014). An exploratory methodology was selected to meet the research objectives of documenting the gap between actual and ideal security policies and procedures within crisis organizations; the gap between crisis organizations who provide services to different categories of victims (e.g. domestic violence, human trafficking, etc.); and the gap across dimensions of security as identified by the NIST CSF. The study also explored whether security preparedness is associated with the application of information security solutions while identifying characteristics of crisis organizations lacking in current research. Challenges did occur when working with organizations in remote locations in the US, but were overcome because of the commitment to this study by representatives at NNEDV, Thorn, and Demand Abolition. As a result, the author was able to enlist a substantive pool of respondents that represent the domains identified for this study.

4.2 Procedures

4.2.1 Survey Development

The survey for this study was modeled using the 2012 survey conducted by the National Network to End Domestic Violence (NNEDV) and the NIST CSF (NIST, 2014). As part of the research protocol, participating organizations were required to agree to an online consent form and commit to answering all questions. The survey was designed using Qualtrics Survey Software (see Appendix C). Throughout this study, there was an emphasis on the intersection of technology, policies, and people as also supported by the

NIST CSF core functions of Identify, Protect, and Respond (NIST, 2014). The functions of the NIST CSF were not included; Detect and Recovery were identified as outside the scope of this study because of the complexity of the subcategories and the level of technical knowledge required for respondents to comprehend (NIST, 2014).

The sections of the NIST CSF included in the draft and final survey development were:

1. Identify (ID):
    a. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy; subcategories 1, 2, 3, 5, and 6.
    b. Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions; subcategories 3 and 4.
    c. Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk; including subcategories 1 and 2.
    d. Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decision; including subcategory 1.

2. Protect (PR):
    a. Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions; including subcategory 1.
    b. Awareness and Training (PR.AT): The organization's personnel and partners are provided with cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements; including subcategories 1 and 2.
    c. Information Protection Processes and Procedures (PR.IP): Security policies (addressing purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets; subcategories 6.
3. Response (RS):
    a. Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events; subcategory 1.

As discussed above, the following functions in the NIST CSF were not included in the final survey; however, they will be incorporated in future research:

4. Identify (ID): Risk Assessment (ID.RA)
5. Protect (PR): Data Security (PR.DS), Maintenance (PR.MA), and Protective Technology (PR.PT)

6. Detect (DE): Anomalies and Events (DE.AE), Security Continuous Monitoring (DE.SC), and Detection Process (DE.DP)
7. Response (RS): Communications (RS.CO), Analysis (RS.AN), Mitigation (RS.MI), and Improvements (RS.IM)
8. Recovery (RC): Recovery Planning (RC.RP), Improvements (RC.IM), and Communications (RC.CO) (NIST, 2014).

4.2.2 Snowball Sample

The sample for this study was identified using the snowball sample method, a technique that helps to reach hard-to-find populations (Atkinson & Flint, 2001). Snowball sampling benefits from established social networks of identified respondents providing a wide set of potential contacts and from being placed within a larger set of connection-tracking methodologies (Spreen, 1992; Thomson, 1997). The sample was identified with the research objectives for this study in mind, along with pre-defined groups and sub-groups as identified outside the view of the author to protect the anonymity of the respondents. The sample for this study was representative of the databases of NNEDV, Thorn, and Demand Abolition, but was not intended to be a pure sample, only the best method of engaging while protecting their identities. NNEDV, Thorn, and Demand Abolition met the criteria for inclusion in this study, as the aim of this study was "primarily explorative, qualitative, and descriptive, then the snowball sample offers practical advantages" (Atkinson and Flint, 2001, pg. 2). Though snowball sampling is typically conducted using interviews, a survey was used for this study. For future research, the snowball sample may be applied to a more formal methodology for making

inferences about the sample of crisis organizations (Faugier & Sergeant, 1997; Snijders, 1992).

4.2.3 Institutional Review Board (IRB)

As stated above, both the draft survey used with the pilot review and the final survey distributed to crisis organizations were constructed using the 2012 NNEDV survey and the NIST CSF (NIST, 2014). To ensure participants in the study were protected, an IRB application and a formal consent form based on the IRB template were submitted for review and approval (see Appendix D). After the completion of the pilot review using the Delphia approach with two rounds of review (Hsu & Sanford, 2007), an amendment to the original application was submitted, reviewed, and approved (see Appendix D).

4.2.4 Pilot Review

The pilot group reviewed the draft of general survey for clarity, consistency, and ease of use for the organizations identified in this study. The pilot review began with the recruitment of 20 subject matter experts spanning information security and crisis organizations (see Appendix E for a list of subject matter experts). These experts were determined by the author, by authorship of journals, and prior identification of expertise in this field. For this process, it was their mission to review the survey for clarity, consistency, and ease of use for the general sample identified in this study. The pilot review used the Delphia approach with two rounds of review (Hsu & Sandford, 2007). Round one commenced by sending an email (see Appendix G for the round one email), which included instructions regarding the role and responsibilities as a pilot survey reviewer, a link to the online survey in Qualtrics, the survey in PDF form (see Appendix

H), and an evaluation sheet attachment to record their feedback (see Appendix F). After acknowledging agreement to the consent form, the participant took the survey and filled out the evaluation form during or immediately following review of the online survey. Pilot reviewers then sent their feedback forms back to the author for compiling and distribution for the second round of review.

For round two, reviewers received a second email (see Appendix I). This included the results from the first round (see Appendix J). At this time in the process, all reviewers were asked to provide additional thoughts and feedback based on the responses of the other participants. When comments from round two were received, participation from the pilot reviewers was complete and the final survey was updated (see Appendix K).

4.2.5 Survey

To initiate the survey, an email invitation (see Appendix L) and link to the online survey were sent to crisis organizations listed in databases owned and managed by NNEDV, Thorn, and Demand Abolition. Based on information provided by these organizations, it was estimated that 700 crisis organizations were contacted for this study. At the start of the survey on Qualtrics, each participant was required to read and agreeing to an online consent form. The respondent was considered the participant. After acknowledging agreement to the online consent form, the participant took the survey. At the end of the survey, the participant's involvement was complete. The data needed to conduct the gap analysis detailed in Chapter 5 were the responses to the survey from participants.

4.3 Participants

The above procedures relied on the open and active participation of the selected pilot review and representatives from NNEDV, Thorn, and Demand Abolition, as well as the survey respondents. If any individual or organization chose not to participate at any point in the study, they could have done so without repercussions. As previously stated, procedures outlined took into consideration the comfort level and time limitation of the crisis organization staff. Individuals and organizations who participated in this study did not receive compensation; however, they were recognized for their participation in the final report.

4.3.1 Pilot Review Participants

Selection of pilot review participants was based on expertise in crisis organizations, information security, NIST CSF, and non-profit organizations. They were contacted via email and telephone to participate as a pilot survey reviewer (see Appendix G). Invitations to 20 potential pilot review participants were sent; of the 20 invitations sent, 13 agreed to participate in the review process (see Appendix E for a list of pilot reviewers). Participants were high or executive-level decision makers in their organizations, therefore they did not require additional permission to participate in this study. Their expertise and opinions were necessary for this initial review of the general survey. The researcher had all necessary contact information of the pilot reviewers and communication throughout this study.

As outlined in the methodology section above, participants in the pilot review were individually invited via email (see Appendix G). The researcher sent an email to each participant with instructions for completing the evaluation, a link to the online

survey, a PDF copy of the final survey (see Appendix K), and the evaluation form (see Appendix F). This email reiterated that participation was voluntary and could be concluded at any time by the participant without repercussion (see Appendix G). The email indicated that there were potential benefits to current and future crisis organizations by assessing the current state of information security against an established framework in information security (see Appendix G). Participants were given 10 business days to respond in round one. For round two, participants were given a deadline to update the original response or provide additional feedback (see Appendix I). No response in round two indicated no change in the participant's initial feedback provided in round one. To initiate round one, participants logged into a survey on Qualtrics. Upon arriving at the Qualtrics site, participants were required to read through the consent form and select that they agreed to the consent form before answering or reviewing any questions in the survey and filling out the evaluation form (see Appendix F).

4.3.2 Survey Participants

The survey participants for this study included US-based crisis organizations providing direct and indirect services to victims of violence. These organizations are owned and managed in databases from NNEDV, Thorn, and Demand Abolition. The inclusion criteria were people employed by direct or coordinated service organizations working with victims of violence identified by NNEDV, Thorn, and Demand Abolition. Representatives from NNEDV, Thorn, and Demand Abolition National facilitated the distribution of the general survey by forwarding via email the invitation to participate and the link to the online survey (see Appendix L). The invitation included instructions for the online survey noting that their participation was voluntary and that they were

welcome to opt out of the survey at any time with no repercussions (see Appendix L). The invitation stated that the study sought input from *organizations working with victims of domestic violence, stalking, and human trafficking in the United States* (see Appendix L). Additional validation if the organization responding was US-based was not conducted for this study as it was foundational in scope. The invitation outlined potential benefits to current and future crisis organizations by identifying the current state of information security with an established framework in cybersecurity (see Appendix L). Two reminder emails were provided to NNEDV, Thorn, and Demand Abolition for their databases (see Appendix L). Based on initial discussions with representatives from these organizations, the total number of survey participants was estimated to be 700 crisis organizations (K. Lee, personal communication, September 2015; L. Treitman, personal communication, September 2015; D. Workman & D. Warren, personal communication, October 2015).

As with pilot reviewers, all survey participants logged into a survey on Qualtrics and were required to read the consent form and select that they agreed to the consent form before answering any questions in the survey.

4.4 Literature and General Media Review

Monitoring research, literature, and general media in the domain of domestic violence, human trafficking, and stalking was conducted and as relates to the objectives of this study. In addition, academic and general media key word and content searches were conducted on the non-profit sector, not specific to crisis organizations, to ensure relevant information within the scope of this study and future research was included. Results from the literature and general media review were reported in Chapter 2.

CHAPTER 5. GAP ANALYSIS AND FINDINGS

The purpose of this study was to identify the current state of information security within crisis organizations by examining the gaps between a theoretical maximum level of information security and the observed level of information security preparedness. This study measured and explored these gaps by looking at absolute and relative levels of information security preparedness using three functions of best practices inspired by a recognized and respected framework – the NIST Cybersecurity Framework (see Appendix B for framework details). To report on these gaps and therefore, identify the current state of information security within crisis organizations, data from survey respondents was gathered using Qualtrics Survey Software (see Appendix N for detailed survey results). The data was then analyzed, in support of the research objectives for this study, in three core areas. First, as a result of the lack of research in this area, the study provided foundational content for this and future research by documenting the characteristics of crisis organizations through an explanatory. Second, a gap analysis was conducted measuring respondent data against an information security preparedness index developed for this study using the NIST Cybersecurity Framework (NIST, 2014). Third, exploratory analysis was also conducted providing additional insights to the current state of information security within crisis organizations again for this study and as a foundation for ongoing research.

5.1 Survey Respondents Summary

As indicated in Chapter 4, the sample for this study was identified using the snowball sample method and support from NNEDV, Thorn, and Demand Abolition. Based on communication with representatives from NNDEV, Thorn, and Demand Abolition, the link to the online survey was distributed the estimated sample of between 500 and 700 crisis organizations, coalitions, agencies, and centers within the US. From this estimated sample, 222 participants clicked on the survey link. Out of those, 221 agreed to the online consent form in question one thereby beginning the survey. One participant opted out of the study for an unknown reason. As a result, the study began with 221 respondents who consented to take the survey. After initial review of the survey data, it was discovered that 63 of the 221 consenting respondents did not answer any of the survey questions and therefore were not included in the analysis. In addition, though 15 respondents who consented to taking the survey did not answer all questions, to support the objectives of this study every answer provided by a consenting respondent was included. Therefore, the sample for this study included survey respondents who consented, but did not answer all questions (15 respondents) plus respondents who consented and answered all questions (143 respondents) for a total of 158 respondents. The forthcoming analysis was based on $N = 158$ possible respondents. Refer to Table 2 for a summary of the number of survey respondents and Appendix M for complete survey respond details.

Table 2. *Survey Respondents Summary*

Survey Activity	Number of Respondents
Clicked on the survey link	222
Selected "Do Not Consent"	1
Selected "Consent"	221
Consented; Did Not Answer Any Questions	63
Consented; Not All Questions Answered	15
Consented; Answered All Survey Questions	143

Note: N = 158 comprised of Consented; not all Questions Answered plus Consented; Answered All Survey Questions

5.2 Characteristics of Crisis Organizations

As a result of the lack of research regarding information security within crisis organizations and the foundational focus of this study, this section examines the characteristics of crisis organizations essential for this and future research. To support the research objective and to examine the factors (e.g. funding, lack of resources, and lack of knowledge) associated with the gap analysis, the analysis incorporated response data from three survey questions. These questions included:

1. What type(s) of victims or survivors does your organization serve?
2. What is the size of your organization?
3. What is the total annual budget of your organization?

5.2.1 Type of Victims Served

First, of the 158 total survey respondents, 157 choose to answer the question, *what type(s) of victims or survivors does your organization serve?* Respondents were provided the opportunity to select all the services that apply through pre-set check box options. There were also offered the opportunity to answer "Other" and provide a filling-in response. Some of pre-set options respondents could choose from included domestic violence, stalking, human trafficking, and sexual abuse. Initial review of the data indicated that out of the 157 respondents, 83.4% (131 respondents) reported servicing

more than one type of victim. In addition, Table 3 illustrates that 96% survey respondents serving victims and survivors of domestic violence with 73% servicing victims of sexual assault and 70% servicing victims of stalking.

Table 3. *Type(s) of Services Provided by Crisis Organizations*

Type of Service(s)	# of Responses	% of Respondents
Domestic Violence	151	96%
Sexual Assault	116	73%
Stalking	111	70%
Human Trafficking	86	54%
Refugee	23	15%
Other	20	13%

Other types of organizations also reported included adult protective services and services for homeless, immigrants, and victims of child sexual abuse (see Appendix N for fill-in response details).

5.2.2 Size of the Organization by Resource Type

The size of crisis organizations participating in the study also provided an important foundational content for this and future research. Survey respondents were asked to identify the size of their organization by if they have full-time employees, part-time employees, and volunteers. Respondent selected the appropriate category(ies) for their organization then were provided an opportunity to specify the number of people in their organization by category. As with organizations who responded to what type of services provided, out of 158 possible respondents, 156 organizations answered this question. Therefore, out of the sample (n = 156), 97% reported having full-time employees, 88% reported having volunteers, and 83% reported part-time employees. Refer to Table 4 for details on responses by type of staff.

Table 4. *Number of Responses by Type of Staff*

	# of Responses	% of Respondents
Full-Time Employees	152	97%
Volunteers	137	88%
Part-Time Employees	129	83%

As illustrated in Table 5, the frequency of respondents who reported having all three categories, full-time, part-time, and volunteers, dominated the results with a total of 118. A minimal number of respondents reported having only full-time (10 respondents) or only part-time (1 respondent) employees. No crisis organizations participating in this study reported being staffed only with volunteers. However, 17 respondents reported having both full-time employees and volunteers with no part-time employees. Refer to Table 5 for details regarding the frequency of responses reporting full-time employees, part-time employees, and volunteers.

Table 5. *Frequency of Responses by Type of Staff*

	Frequency of Score (*f*)	Relative Frequency (*f*/*n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
All	117	0.74	74.05	74.05
FT Only	10	0.06	6.33	80.38
PT Only	1	0.01	0.63	81.01
Volunteers Only	0	0.00	0.00	81.01
FT and PT	8	0.05	5.06	86.08
FT and Volunteers	17	0.11	10.76	96.84
PT and Volunteers	3	0.02	1.90	98.73
	156	1.00	100.00	

Further analysis of the number (fill-in) of full-time employees, part-time employees, and volunteers reported by survey respondents provided additional explanatory data for this and future studies. Out of the sample (n = 156) crisis organizations 154 organizations completed the fill-in section of this question. The

maximum number of employees and volunteers reported was 900 with the minimum being 1. The first and third interquartile range for this data reported 17 for the first quartile and 81 for the third quartile with no outliers observed. Additional observation of the data revealed that 90 crisis organizations reported having a total organizational size of 50 employees or less (see Figure 2). Of 154 organizations who responded, 19% (30 respondents) reported an organizational size greater than 100 combined staff including full-time employees, part-time employees, and volunteers illustrating that the majority of crisis organizations in this study have a staff of less than 100.

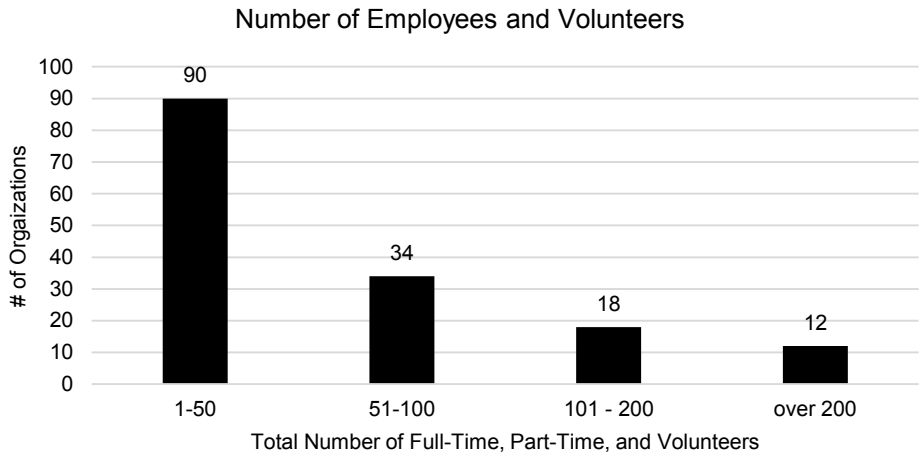


Figure 2. The size of crisis organizations as organized by total number of full-time employees, part-time employees, and volunteers.

5.2.3 Budget Size

The final characteristic of crisis organizations examined was the size of budgets within crisis organizations. Responses from the survey question, *what is the total annual budget for your organization*, provided an important initial look at the amount of financial resources available to crisis organizations and how it compares with information

security preparedness. Respondents were required to select only one budget range. Of the sample (N = 158), 55 (35%) reported annual budgets between $1,000,000 and $4,999,999 with 25 (16%) reporting between $500,000 and $999,999. In addition, although all respondents in the sample answered this question, 26 (16%) respondents selected "Do Not Know," a point that will be addressed further in the discussion section of this study. Refer to Table 6 for a summary annual budget size from all respondents.

Table 6. *Annual Budget Size*

	# of Responses	% of Respondents
$1,000,000- $4,999,999	55	35%
Do Not Know	26	16%
$500,000 - $999,999	25	16%
$150,000 - $349,999	15	9%
$350,000 - $499,999	11	7%
$75,000 - $149,000	11	7%
Greater than $5,000,000	9	6%
Less than $75,000	6	4%
Total	158	100%

In summary, the data provided by survey respondents with regards to the type(s) of services provided by the organization, the size of the organization based on full-time employees, part-time employees, and volunteers, and annual budget allowed for the examination of these factors against the information security preparedness index and exploratory analysis. However, it also set the initial baseline for understanding the characteristics of crisis organizations while providing the needed foundation for future research.

5.2.4 Discussion

The analysis of crisis organizations characteristics in this study provided a needed foundation and the initial insights for future research on information security within crisis

organizations. From this analysis, a few pertinent insights emerged for continued discussion and research. For example, 63 out of 221 respondents clicked consent, but did not continue with the survey. This might suggest a few areas, such as survey length, technical terminology, and concern over the subject matter, to investigate prior to future surveys with these type of organizations. Next, with 83.4% (131 out of 158 respondents) reporting that they service more than one type of victim, it is important to consider how the different characteristics of these victims and the services they need may or may not impact the level of information security preparedness across the organization. In addition, it was observed that four organizations reported being run by part-time employees or part-time employees and volunteers calling into consideration the information security preparedness when no full-time employees are on staff. Last, after analyzing responses from the question pertaining to budget size, it is important to note 26 (16%) respondents selected "Do Not Know" as their response. These responses call into question whether the person completing the survey had access to budget information or chose not to answer the question for other reasons.

5.3 Gap Analysis on Information Security Preparedness Index

To create context for the analysis and to measure the gap of information security preparedness within crisis organizations, an index for information security preparedness was developed. The index provided a tool for this study and a foundation for future research to identify gaps between the current state for information security policies and procedures within crisis organizations and the ideal state by using best practices and functions, Identify and Protect, from NIST Cybersecurity Framework (see Appendix B framework details). Based on the survey questions created for this study the ideal state of

information security equated to a score of 23. Though, the NIST CSF function, Respond, was used in the survey, the results were determined, by the author, to be more suitable for the exploratory section of this study. In addition, improving the current information security preparedness index, as well as expanding it to include all five functions of the NIST Cybersecurity Framework, could be a focal point for future research in this area.

When reporting the results of the survey, the researcher used the information security preparedness index, which was organized to align with three out of five of the research objectives for this study. First, responses from all consenting respondents were measured using the index to document the gap between actual and ideal state of information security policies and procedures as outlined by the NIST CSF (NIST, 2014). Second, survey responses were categorized to examine the gap crisis organizations who provide services to victims within two categories as determined by responses to the survey question, *what type(s) of victims or survivors does your organization serve* (see Appendix N for survey details). These categories included crisis organizations who provide services to victims of domestic violence and human trafficking and those who provide services to domestic violence but not human trafficking victims. Last, survey responses were examined to document the gap of information security preparedness across different dimensions of information security as outlined in Identify and Protect functions of the NIST CSF (see Appendix B for a complete summary of the NIST Cybersecurity Framework functions, categories, and subcategories).

Last, scores calculated using the information security preparedness index reported frequency, mean (*M*), and median. As indicated in the detail below, reports on frequency within the data provided descriptors to identify where on the index scale crisis

organizations scored. Also, mean (*M*) and median provided indicators of central tendency to help identify outliers. Future research studies would improve the survey and resulting data to allow for the expanded use of statistical tools in identifying crisis organizations who improve or weaken their information security preparedness index over time and for what reasons.

5.3.1 Information Security Preparedness for All Respondents

As stated above, the information security preparedness index was used to measure the current state of information security across all consenting respondents ($N = 158$). Based on the survey questions aligned with the index, a score for information security preparedness was 23 with a mean (*M*) 12. The range of possible scores was zero to 23 with observed scores ranging from one to 23.

Across the total sample of respondents ($N = 158$), two respondents scored a score of 23 and one respondent scored a low of one. No crisis organizations participating in this study scored zero for information security preparedness. Mean (*M*) and median scores of 12 were reported across all respondents. As a result, 156 respondents reported a score less than the ideal state of information security preparedness. In addition, 49% (81) of respondents reporting better than average scores. Further examination of scores across the sample indicated that 74% of respondents scored between 18 and seven, with 11 respondents scoring at the mean (*M*) of 12. The interquartile range (Q3 – Q2) of 54.4% was defined between a score of 17 and nine with no outliers. Refer to Table 7 for information security preparedness scores for all consenting respondents.

Table 7. *Information Security Preparedness Index by All Consenting Survey Respondents*

Score	Frequency of Score (*f*)	Relative Frequency (*f*/*n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
23	2	0.01	1.27	1.27
22	1	0.01	0.63	1.90
21	9	0.06	5.70	7.59
20	8	0.05	5.06	12.66
19	5	0.03	3.16	15.82
18	9	0.06	5.70	21.52
17	12	0.08	7.59	29.11
16	12	0.08	7.59	36.71
15	8	0.05	5.06	41.77
14	7	0.04	4.43	46.20
13	5	0.03	3.16	49.37
12*	11	0.07	6.96	56.33
11	11	0.07	6.96	63.29
10	10	0.06	6.33	69.62
9	10	0.06	6.33	75.95
8	10	0.06	6.33	82.28
7	12	0.08	7.59	89.87
6	4	0.03	2.53	92.41
5	4	0.03	2.53	94.94
4	4	0.03	2.53	97.47
3	2	0.01	1.27	98.73
2	1	0.01	0.63	99.37
1	1	0.01	0.63	100.00
Total	158	1.00	100.00	

**mean (M) and median score*

Figure 3 represents the frequency the all consenting respondents ($N = 158$) scored by the information security index scores. This figures illustrates the greatest number of respondents (12) reporting an information security preparedness score of 17, 16, or seven. The fewest number of respondents reported scores on the ends of the scale including scores 23, 22, three, two, and one. Although the data does not indicate a large skew, the mean (M) of 13 and median of 12 are not equal. Future research would identify how

changes in the information security preparedness index would or would not affect the mean (*M*) and median.

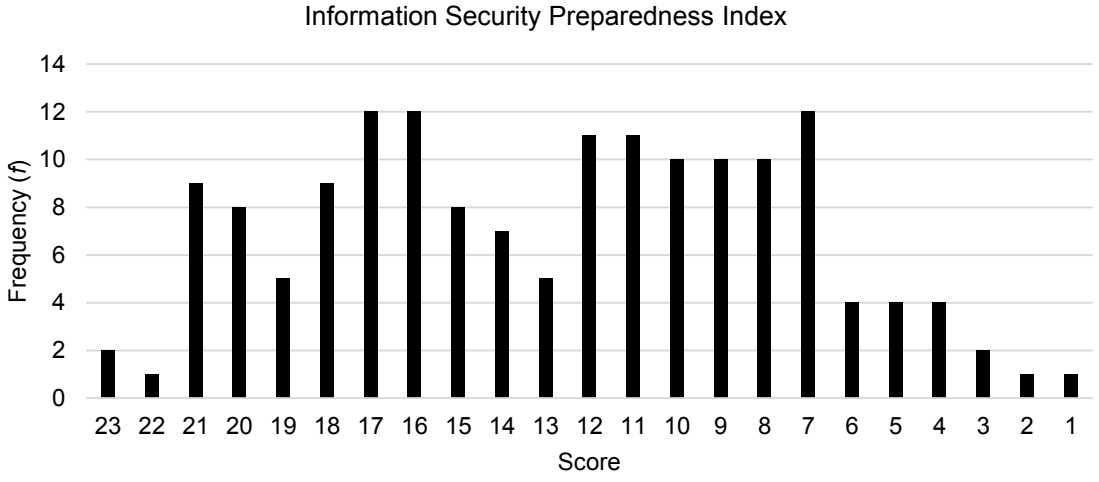


Figure 3. Information Security Preparedness of All Consenting Respondents. This figure illustrates the frequency of respondents by index score.

5.3.2 Information Security Preparedness by Category

Additional analysis using the information security preparedness index was conducted by categorizing the sample. This analysis utilized responses from survey question, *what type(s) of victims or survivors does your organization serve*, to determine categories in alignment with the objective of this study to document the gap between crisis organizations who provide services to different categories of victims. As a result, two primary categories of crisis organizations were identified for further analysis. The first category included crisis organizations who provide services to victims of domestic violence and human trafficking – $n = 81$ or 52% of the total sample. The second category was comprised of crisis organizations who provide services to domestic violence not including human trafficking victims – $n = 70$ or 45% of total sample. The information

security preparedness indices for the remaining six organizations are included in the discussion section.

5.3.2.1 Domestic Violence and Human Trafficking

In conjunction with the data of the entire sample, a score for information security preparedness for crisis organizations servicing domestic violence victims and human trafficking victims was 23 with a mean (*M*) of 12. The range for scores was zero to 23 with observed scores ranging from one to 23. Similar to results from all respondents, respondents in this category (*n* = 81) identified two crisis organizations who scored a score of 23 and one scoring a low of one. No crisis organizations participating in this study scored zero for information security preparedness. Similar to all respondents, a mean (*M*) and median score identical at 13 were reported. Also, observed was a gap of 76 respondents reported a score less than ideal state for information security for organizations servicing victims of domestic violence and human trafficking.

During further analysis of the data revealed 76% of the sample (*n* = 18) scored between 18 and seven, with four respondents scoring at the mean (*M*) of 13. In addition, the interquartile range (Q3 – Q2) of 30% was defined between a score of 17 and 13. Refer to Table 8 for information security preparedness scores for respondents servicing domestic violence victims including human trafficking victims.

Table 8. *Information Security Preparedness Index: Servicing Victims of Domestic Violence and Human Trafficking*

Security Preparedness Index	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
23	2	0.02	2.47	2.47
22	1	0.01	1.23	3.70
21	2	0.02	2.47	6.17
20	4	0.05	4.94	11.11
19	3	0.04	3.70	14.81
18	5	0.06	6.17	20.99
17	6	0.07	7.41	28.40
16	6	0.07	7.41	35.80
15	5	0.06	6.17	41.98
14	4	0.05	4.94	46.91
13*	4	0.05	4.94	51.85
12	4	0.05	4.94	56.79
11	7	0.09	8.64	65.43
10	8	0.10	9.88	75.31
9	4	0.05	4.94	80.25
8	5	0.06	6.17	86.42
7	4	0.05	4.94	91.36
6	0	0.00	0.00	91.36
5	4	0.05	4.94	96.30
4	0	0.00	0.00	96.30
3	1	0.01	1.23	97.53
2	1	0.01	1.23	98.77
1	1	0.01	1.23	100.00
Total	81	1.00	100.00	

**mean (M) and median score*

Figure 4 represents the frequency by information security preparedness scores within this category. The highest frequency reported eight crisis organizations scoring a security preparedness index of 10; with 38 (46%) of organizations scoring above the mean (*M*) of 13.

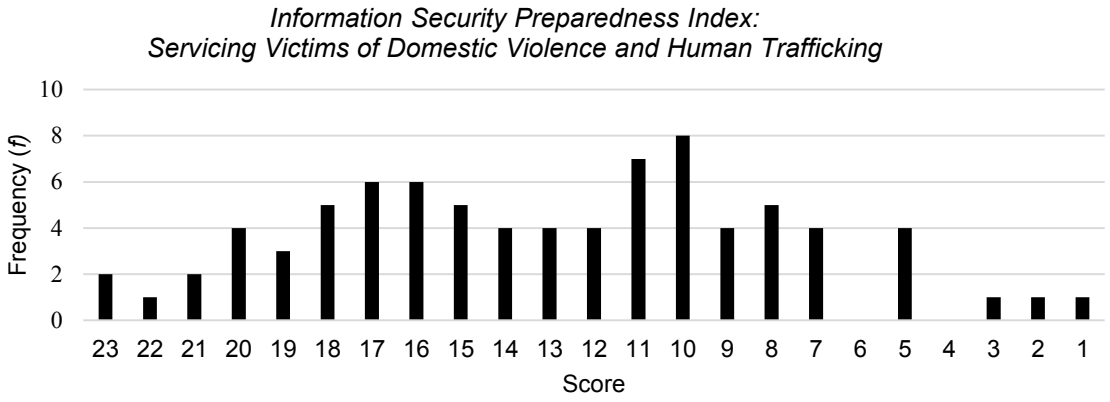


Figure 4. Information security preparedness of organizations servicing victims of domestic violence and human trafficking. This figure illustrates the frequency of respondents by index score.

5.3.2.2 Domestic Violence not including Human Trafficking

The analysis of the second category, crisis organizations servicing victims of domestic violence not including human trafficking victims, had a score for information security preparedness of 23 with a mean (*M*) of 12. As with the above category and the analysis of all respondents, the range for scores is zero to 23 with observed scores ranging from three to 21. Across the total sample ($n = 70$) of respondents in this category, the highest preparedness score reported was not ideal at 21 and was reported by seven crisis organizations. The gap was all ($n = 70$) respondents do not fall within the ideal state of information security preparedness. In comparison, the lowest score reported by this category of respondents was three by one respondent. No crisis organizations participating in this study scored zero for information security preparedness. Results reported a mean (*M*) and median of 12.

Although the index revealed respondent scores across a range of 21 to three, the largest number of respondents (7) was observed across three different scores: the highest reported score of 21, the mean (*M*) of 12, and a score of seven. A total of 32 (45%) of respondents scored above the mean (*M*). In addition, the data displays the interquartile range (Q3 – Q1) of 57% was defined between a score of 17 and eight. Refer to Table 9 for information security preparedness scores for respondents servicing domestic violence victims not including human trafficking victims.

Table 9. *Information Security Preparedness Index: Servicing Victims of Domestic Violence not including Human Trafficking*

Score	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
23	0	0.00	0.00	0.00
22	0	0.00	0.00	0.00
21	7	0.10	10.00	10.00
20	3	0.04	4.29	14.29
19	2	0.03	2.86	17.14
18	3	0.04	4.29	21.43
17	6	0.09	8.57	30.00
16	5	0.07	7.14	37.14
15	2	0.03	2.86	40.00
14	3	0.04	4.29	44.29
13	1	0.01	1.43	45.71
12*	7	0.10	10.00	55.71
11	4	0.06	5.71	61.43
10	2	0.03	2.86	64.29
9	5	0.07	7.14	71.43
8	5	0.07	7.14	78.57
7	7	0.10	10.00	88.57
6	4	0.06	5.71	94.29
5	0	0.00	0.00	94.29
4	3	0.04	4.29	98.57
3	1	0.01	1.43	100.00
2	0	0.00	0.00	100.00
1	0	0.00	0.00	100.00
Total	70	1.00	100.00	

**mean (M) and median score*

Figure 5 represents the frequency sample (n = 70) who provide services to domestic violence victims not including human trafficking victims. As indicated above, the greatest frequencies (7) were reported across three scores, 21, 12, and seven were the fewest reporting a score of 13 and three. No organizations in this category scored a 23, 22, five, two, or one for information security preparedness.

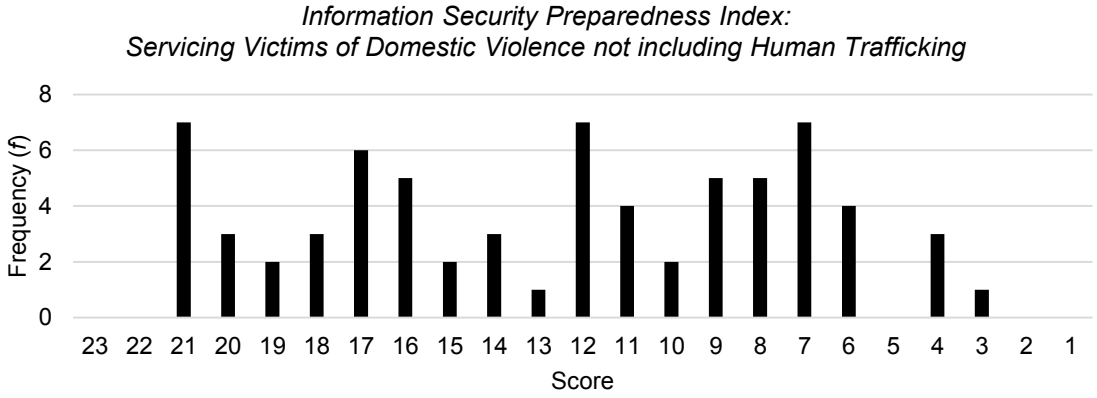


Figure 5. Information security preparedness of organizations servicing victims of domestic violence not including human trafficking. This figure illustrates the frequency of respondents by index score.

5.3.2.3 Discussion

The results documented above provide an initial view into the gap between the ideal state of information security preparedness and crisis organizations who provide services to different categories of victims. To summarize, the boxplot diagram in Figure 6 illustrates the upper and lower bounds of the interquartile range for each of the three data sets analyzed above. The lower bounds, upper bounds, and median of the all respondents and organizations servicing domestic violence and human trafficking were identical with

one possible outlier at the lower bound. While the lower bound and median for respondents servicing victims of domestic violence but not human trafficking were different. The mean (*M*) for all respondents and crisis organizations servicing victims of domestic violence not human trafficking was 12, while the mean (*M*) for crisis organizations servicing victims of domestic violence and human trafficking was 13.

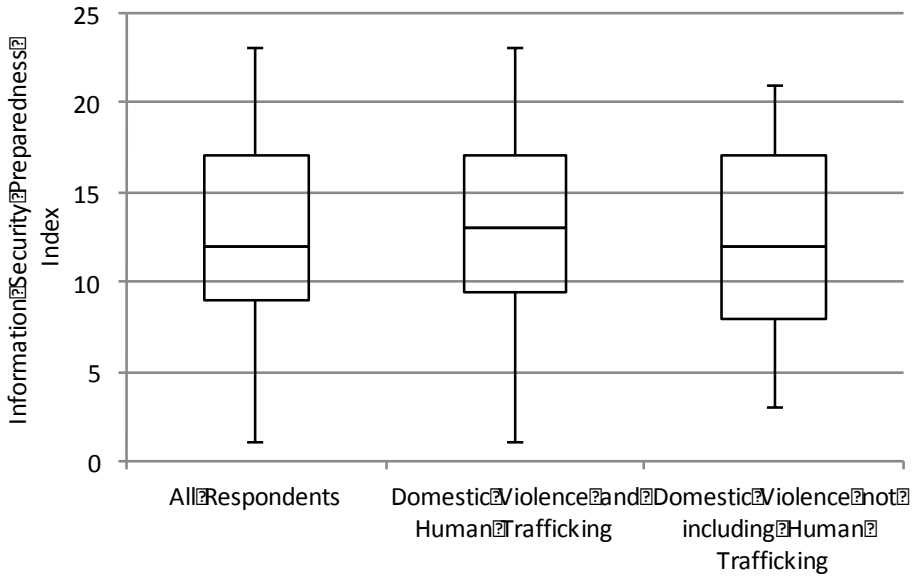


Figure 6. Interquartile range of the information security preparedness index for all respondents, organizations working with victims of domestic violence and human trafficking, and organizations working with domestic violence not including human trafficking.

5.3.3 Dimensions of Security in the NIST Cybersecurity Framework

This section analyzes the survey data to document the gap across dimensions of information security preparedness as outlined by the NIST CSF (NIST, 2014). Survey results from this study were organized by NIST CSF function, category, and sub-

category. Refer to Appendix L for a details on how survey questions were mapped to the NIST CSF by function, category, and sub-category. In addition, as addressed in Chapter 1 and Chapter 4, three out of five core functions in the NIST CSF were selected for this study – Identify, Protect, and Response. Out of the 45 survey questions 28 questions map to the NIST CSF. The remaining 17 survey questions were developed using the 2012 NNEDV survey and for general purpose use (see Appendix C for a table outlining the source of each survey question).

For the gap analysis survey data from the Identify and Protect functions were used. Survey data from the Response function was identified relevant for the exploratory analysis section of this study and has been included there. Consistent the above sections, survey data from the Identify and Protect functions were analyzed by all consenting respondents then also by organizations who provide services to domestic violence and human trafficking victims and organizations who provide services to victims of domestic violence not including human trafficking.

5.3.3.1 Identify Function

The objective of the NIST CSF function, Identify, was to "develop the organization understanding to manage cybersecurity risk to systems, assets, data, and capabilities" (NIST, 2014, pg. 6). A necessary first step in any process is to identify what is known today, therefore, this first function helps organizations to identify critical assets, operations, and areas where risk may exist. The Identify function is comprised of five categories: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy (NIST, 2014). Beyond these five categories is a total of

24 subcategories (NIST, 2104). In concurrence with organizations and industry experts who have used the NIST CSF, the Identify function is an important initial step in understanding information security in relationship to the holistic business environment (Atlas Vault, 2016). “This step is the pivot upon which the other four functions work” (Atlas Vault, 2016, pg. n/a). In addition, for the purpose of this study, four of the five categories from the Identify function were included: Asset Management, Business Environment, Governance, and Risk Management Strategy (NIST, 2014). A map of survey questions, NIST functions and categories, along with corresponding appendixes can be found in Appendix M.

As with the above, a frequency analysis on the survey data corresponding to the Identify function was conducted. This analysis included responses from 16 out of the 21 survey questions identified in the Identify function. Data from two out of the 21 survey questions are addressed in the exploratory analysis. Important to note, three questions were not included in the frequency analysis as responses are contingent upon the question previous. Data from these questions may be used in future research initiatives. Refer to Table 10 and the corresponding notations for further detail on the survey questions mapped to the Identify function, categories, and subcategories.

Table 10. *Identify Function Categories Mapped to Survey Questions*

Category	Survey question
Id.am-1: physical devices and systems within the organization are inventoried.	Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies belonging to the organization? *
	Do you know if these items are insured against theft or loss?
Id.am-2: software platforms and applications within the organization are inventoried.	Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies belonging to the organization?*
	Does your organization currently use any of the following security technologies?
	Is the software used by your organization inventoried?
Id.am-3: organizational communication and data flows are mapped.	Does your staff access internal electronic documents from outside the premises?*
	Who in your organization is responsible for managing the organization's social media channel(s)?
	Does your organization have human resources policies regarding social media use by the following
	Does your organization have policies for information security?*
Id.am-5: resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value.	Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies belonging to the organization?*
	Has your organization identified what hardware and software are critical to your operations?
Id.am-6: cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Who is responsible for information security for the organization?*
	Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures?
Id.be-3: priorities for organizational mission, objectives, and activities are established and communicated.	Where is the mission of your organization posted?***
Id.be-4: dependencies and critical functions for delivery of critical services are established.	Does your organization have policies or documented policies for power or internet outages?
	Does your organization have policies for physical security?*
	Does your organization have policies for information security?*
	If yes, which technologies do these policies include?**

Table 10 continued

Id.gv-1: organizational information security policy is established.	Does your staff access internal electronic documents from outside the premises?* Does your organization have policies for information security?* If yes, which technologies do these policies include?** Does your organization have policies for physical security?*
Id.gv-2: information security roles & responsibilities are coordinated and aligned with internal roles and external partners.	Who is responsible for information security for the organization?*
Id.rm-1: risk management processes are established, managed, and agreed to by organizational stakeholders.	Has your organization identified areas or practices that may be attractive targets or vulnerable for attack or breach? Has your organization experienced a cybersecurity attack or breach?*** Does your organization consider itself prepared to handle a cybersecurity breach or attack? Has your organization conducted information security workshops or training with staff, volunteers, and other stakeholders? If yes or plan to soon, who will conduct the training?**

Notes:

**survey questions that map to more than one category within the identify function.*
*** survey questions not included in the information security preparedness index because response data is contingent upon the response previous.*
****survey questions not included in the gap analysis – included in the exploratory analysis.*

5.3.3.1.1 Identify Function for All Respondents

The information security preparedness index was used to measure the current state of information security within the boundaries of the NIST CSF Identify function across all consenting respondents ($N = 158$). Based on the survey questions aligned with NIST CSF Identify function, categories, and subcategories, a score for information security preparedness was 16. The range of possible scores was zero to 16 with the observed scores ranging from one to 16.

Across the total sample ($N = 158$), three respondents scored a score of 16 and one respondent scoring the lowest score of one. Thirteen crisis organizations reported scores at the mean (M) and median of nine with 46% (74) scoring above the mean (M). No crisis organizations participating in this study scored zero for information security preparedness. The gap revealed 155 respondents reporting a score less than ideal for information security preparedness. Further analysis of the results showed 72% (115) of the sample ($N = 158$) scored between 13 and five, with the fewest respondents scoring at the lower end of the index. The interquartile range (Q3 – Q2) of 54.4% was defined between a score of 12 and nine and no outliers. Refer to Table 11 for information security preparedness scores for all consenting respondents.

Table 11. *Information Security Preparedness Index, Identify Function: All Consenting Respondents*

Score	Frequency of Score (*f*)	Relative Frequency (*f*/*n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
16	3	0.02	1.90	1.90
15	6	0.04	3.80	5.70
14	7	0.04	4.43	10.13
13	15	0.09	9.49	19.62
12	15	0.09	9.49	29.11
11	15	0.09	9.49	38.61
10	13	0.08	8.23	46.84
9*	13	0.08	8.23	55.06
8	17	0.11	10.76	65.82
7	16	0.10	10.13	75.95
6	13	0.08	8.23	84.18
5	13	0.08	8.23	92.41
4	8	0.05	5.06	97.47
3	2	0.01	1.27	98.73
2	1	0.01	0.63	99.37
1	1	0.01	0.63	100.00
Total	158	1.00	100.00	

**mean (M) and median score*

Figure 7 represents the frequency scores within the Identify function across all survey respondents ($N = 158$). The greatest number of respondents (17) reported a score of eight, one point below the mean (M) of nine. Also illustrated within Figure 7 are the majority of the scores being reported between five and 13

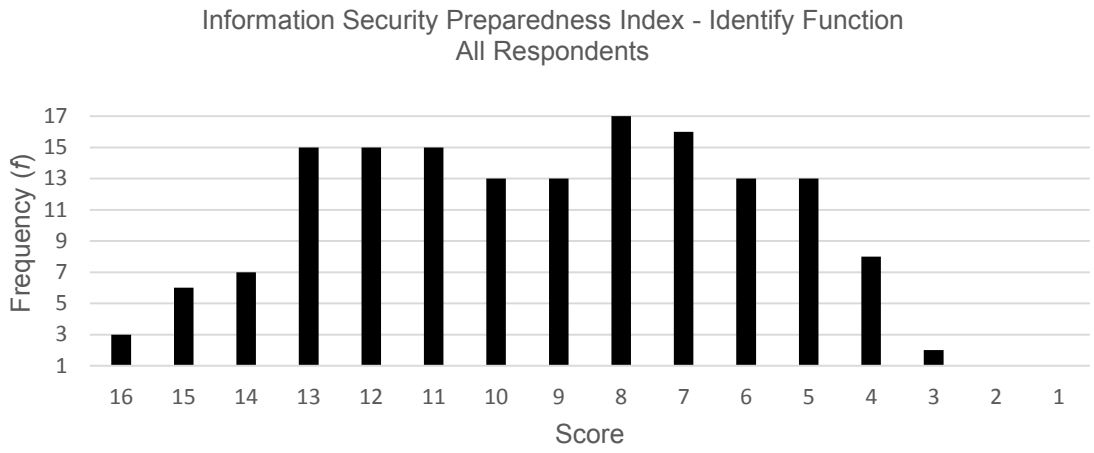


Figure 7. Information security preparedness by the Identify Function of all respondents. This figure illustrates the frequency of respondents by index score.

5.3.3.1.2 Domestic Violence and Human Trafficking

Continuing within the Identify function, frequency analysis was conducted across organizations servicing victims of domestic violence and human trafficking and organizations who services domestic violence victims and not human trafficking victims. The results observed between the entire sample and organizations servicing victims of domestic violence and human trafficking were similar. Though the number of respondents who service victims of domestic violence and human trafficking was 81, the highest possible score (16) was observed with two respondents. The majority of respondents (11) scored a preparedness index of 13 (see Table 12). The mean (M) score

of nine was reported by nine crisis organizations. The mean (*M*) and median were equal (9) across the sample. Similar to the all respondents' sample, results from organizations servicing victims of domestic violence and human trafficking reported displayed an interquartile range (Q3 – Q2) of 33.3% was defined between a score of 12 and nine.

Table 12. *Information Security Preparedness Index, Identify Function: Servicing Victims of Domestic Violence including Human Trafficking*

Score	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
16	2	0.02	2.47	2.47
15	2	0.02	2.47	4.94
14	3	0.04	3.70	8.64
13	11	0.14	13.58	22.22
12	7	0.09	8.64	30.86
11	6	0.07	7.41	38.27
10	5	0.06	6.17	44.44
9*	9	0.11	11.11	55.56
8	9	0.11	11.11	66.67
7	10	0.12	12.35	79.01
6	8	0.10	9.88	88.89
5	4	0.05	4.94	93.83
4	2	0.02	2.47	96.30
3	1	0.01	1.23	97.53
2	1	0.01	1.23	98.77
1	1	0.01	1.23	100.00
Total	81	1.00	100.00	

**mean (M) and median score*

The greatest number of respondents (11) reported a score of 13, one point below the mean (*M*) of nine as illustrated in Figure 8. However, respondents in the category reported scores across the index.

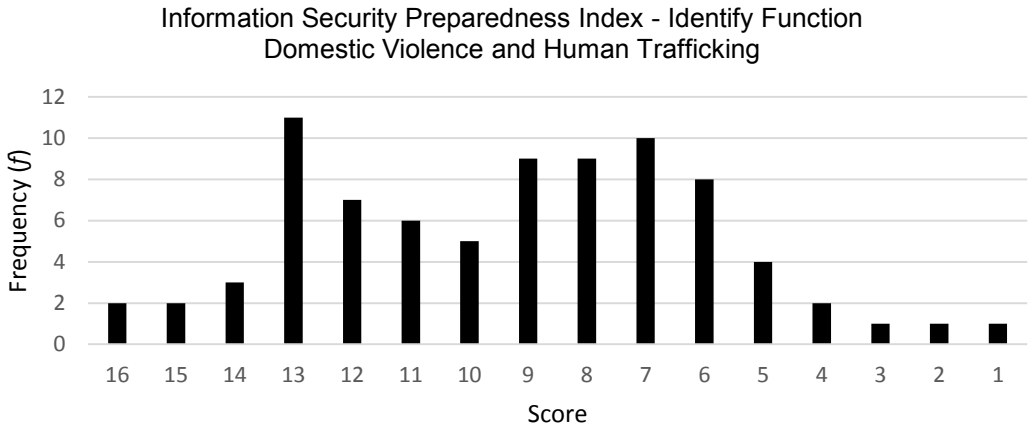


Figure 8. Information security preparedness by the Identify Function for crisis organizations servicing victims of domestic violence and human trafficking.

5.3.3.1.3 Domestic Violence not including Human Trafficking

The final gap analysis within the Identify function was conducted by observing organizations who services domestic violence victims and not human trafficking victims. As with the above analysis, the total number of respondents for this analysis was $N = 70$ and an ideal information security preparedness score of 16. The highest possible score (16) was observed with one respondent with the lowest score reported being three. The mean (M) score of nine was reported by few crisis organizations (4) than the categories above. In addition, the mean (M) (9) and median (10) were not equal therefore indicating a small skew in the distribution. No other distributions in the study were skewed. In addition, the frequency scores were distributed with the largest respondents scoring 11 or 5 for information security preparedness (see Table 13). The data also displayed an interquartile range (Q3 – Q2) of 38%, which was defined between a score of 12 and 9.5.

Table 13. *Information Security Preparedness Index, Identify Function: Servicing Victims of Domestic Violence not including Human Trafficking*

Score	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
16	1	0.01	1.43	1.43
15	4	0.06	5.71	7.14
14	4	0.06	5.71	12.86
13	3	0.04	4.29	17.14
12	7	0.10	10.00	27.14
11	9	0.13	12.86	40.00
10**	7	0.10	10.00	50.00
9*	4	0.06	5.71	55.71
8	6	0.09	8.57	64.29
7	5	0.07	7.14	71.43
6	5	0.07	7.14	78.57
5	9	0.13	12.86	91.43
4	5	0.07	7.14	98.57
3	1	0.01	1.43	100.00
2	0	0.00	0.00	100.00
1	0	0.00	0.00	100.00
Total	70	1.00	100.00	

**mean (M) **median score*

Last, as illustrated in Figure 9, the greatest number of respondents (9) reported scores of five and 11. No respondents within this category scored below an information security preparedness score of three. As stated above, the distribution of this sample shows a slight skew with the mean (*M*) (9) and median (10) not being equal.

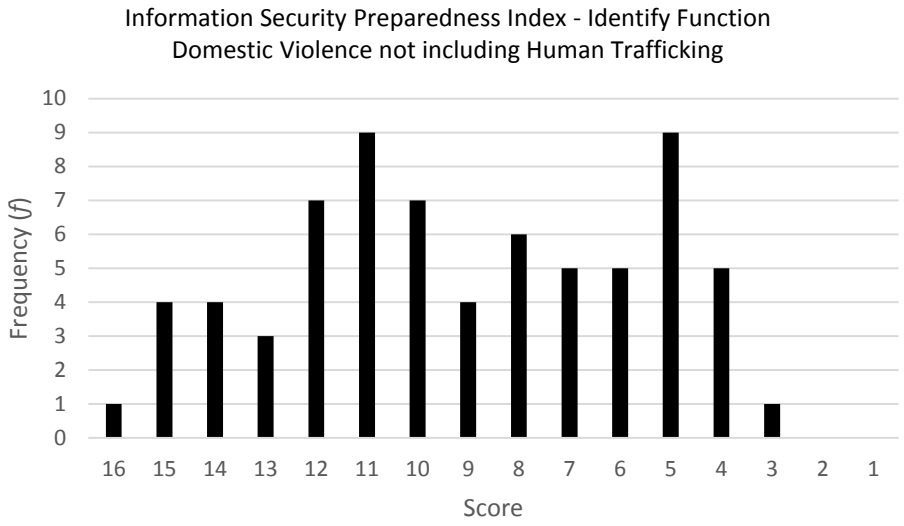


Figure 9. Information security preparedness by the Identify Function for crisis organizations servicing victims of domestic violence not including human trafficking.

The Identify function within the NIST CSF helps organizations identify critical assets, operations, and areas where risk may exist. To summarize, the boxplot diagram (Figure 10) illustrates the upper and lower bounds of the interquartile range for each of the three categories reporting information security preparedness within the Identify function. The lower bounds, upper bounds, and median of the all respondents and organizations servicing domestic violence and human trafficking were identical with one possible outlier at the lower bound. In addition, the mean (*M*) across all categories was consistent at nine, while the median for crisis organizations servicing victims of domestic violence not including human trafficking reported a 10. As a result, the mean (*M*) and median for crisis organizations servicing victims of domestic violence not including human trafficking were not equal indicating a skewed distribution.

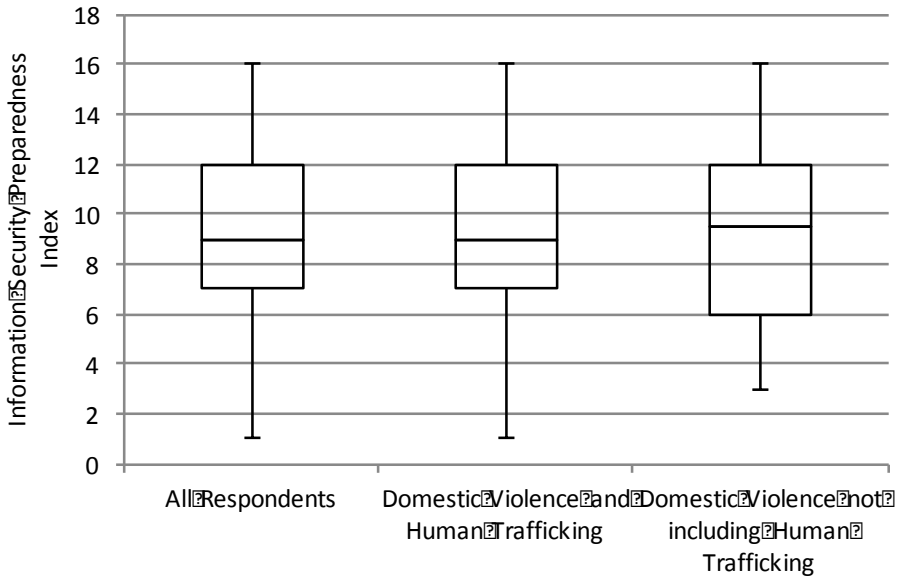


Figure 10. Interquartile range of the information security preparedness index based on the NIST CSF Identify function.

5.3.3.2 Protect Function

The next core function of the NIST Cybersecurity Framework included in this study is Protect (PR). The objective of the Protect (PR) function is to "guide organizations in the development and implementation of appropriate safeguards, prioritized through the organization's risk management process, and to ensure delivery of critical infrastructure services" (NIST, 2014, pg. 6). The Protect function includes categories and subcategories addressing Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Protective Technology (NIST, 2014). For the purpose of this study, the Access Control and Awareness and Training categories were included (NIST, 2014). A map of survey questions, NIST functions, and categories along with corresponding appendices is in Appendix M.

As with the analysis of questions mapping to the Identify function, a frequency analysis on the survey data corresponding to the Protect function was conducted. This analysis included responses from 10 out of the 11 survey questions identified in the Protect function. Data from one question is addressed in the exploratory analysis. Refer to Table 14 and the corresponding notations for further detail on the survey questions mapped to the Protect function, categories, and subcategories.

Table 14. *Protect Function Categories Mapped to Survey Questions*

Category	Survey Question
PR.AC-1: IDENTITIES AND CREDENTIALS ARE MANAGED FOR AUTHORIZED DEVICES AND USERS.	Does your organization have policies for information security? Does your organization document who has access to sensitive files, databases, and other electronic information? How is access to electronic files containing sensitive information stored within your organization protected?*
PR.AT-1: ALL USERS ARE INFORMED AND TRAINED	Has your organization conducted information security workshops or training with staff, volunteers, and other stakeholders? Does your organization inform or train new employees about information security policies and procedures? Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures? If your organization does use third-party vendors, do they inform you of their information security policies and procedures?
PR.AT-2: PRIVILEGED USERS UNDERSTAND ROLES AND RESPONSIBILITIES.	Who in your organization is responsible for the legal requirements for information security? Are the legal requirements listed in Question 28 regarding information security understood by those responsible?
PR.IP-6: DATA SS DESTROYED ACCORDING TO POLICY.	Does your organization have policies and procedures for the destruction of electronic documents? Does your organization have policies and procedures for the destruction of storage devices? (e.g. DVDs, CDs, thumb drives, etc.)

Notes: Survey questions not included in the gap analysis – included in the exploratory analysis.*

5.3.3.2.1 All Respondents

The NIST CSF Protect function was used in the development of the information security preparedness index to measure the current state of information security across all consenting respondents (N = 158). A score for information security preparedness through analysis of just the survey questions corresponding to the NIST CSF Protect function, categories, and subcategories was 10 with a mean (M) 5. The observed range for scores across all respondents was zero to 10.

In comparison to the analysis conducted above, the greatest number of respondents reporting an information security preparedness score was reported in the Protect function. However, results also reported the greatest number of respondents scoring lowest score of zero. Across the total sample (N = 158) of respondents, seven scored a score of 10 and 12 respondent scoring a minimal score of zero. A total of 151 respondents reported a score less than ideal resulting in a gap. Unlike other frequency analysis in this study, the number of respondents across preparedness scores less than 10 were well distributed with greatest number of respondents scored 19. The interquartile range (Q3 – Q2) of 37.9% was defined between a score of eight and five. Refer to Table 15 for information security preparedness scores for all consenting respondents.

Table 15. *Information Security Preparedness Index, Protect Function*

Score	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
10	7	0.04	4.43	4.43
9	19	0.12	12.03	16.46
8	16	0.10	10.13	26.58
7	16	0.10	10.13	36.71
6	16	0.10	10.13	46.84
5*	12	0.08	7.59	54.43
4	17	0.11	10.76	65.19
3	12	0.08	7.59	72.78
2	15	0.09	9.49	82.28
1	16	0.10	10.13	92.41
0	12	0.08	7.59	100.00
Total	158	1.00	100.00	

**mean (M) and median score*

Figure 11 identifies the greatest number of respondents (19) reported close to a score for the Protect function (10) with a score of nine. Unlike the previous analysis, 12 crisis organizations scored the lowest at zero. Mean (*M*) and median scores were reported equal at 5 across the sample.

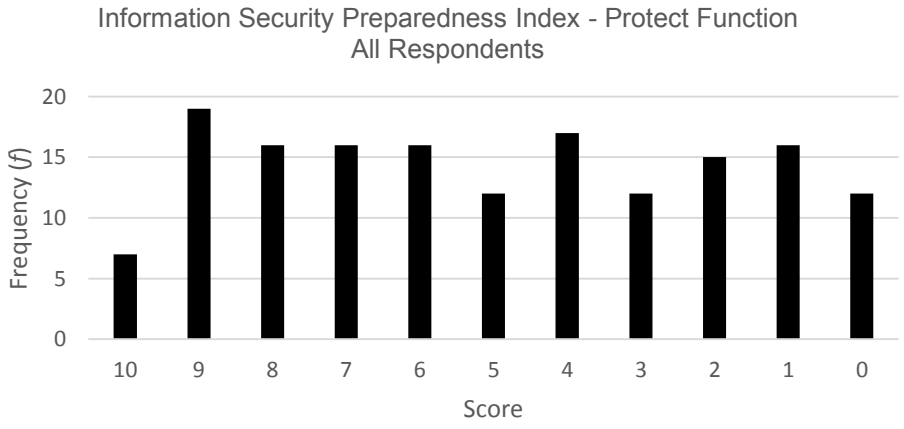


Figure 11. Information security preparedness by the Protect function including all survey respondents.

5.3.3.2.2 Domestic Violence and Human Trafficking Victims

The frequency analysis was also conducted for survey questions that mapped to the NIST CSF Protect function across organizations servicing victims of domestic violence and human trafficking. The results observed between the entire sample (N = 158) and organizations servicing victims of domestic violence not including human trafficking (n = 81) were similar. The highest possible score for information security preparedness (10) was observed by three respondents. However, the majority of respondents (12) scored a preparedness of six; close to the mean (M) of 5 (see Table 16). The interquartile range (Q3 – Q2) of 34.5% was defined between a score of seven and five with no visible outliers.

Table 16. *Information Security Preparedness Index – Protect Function*

Score	Frequency of Score (f)	Relative Frequency (f/n)	Percentage Frequency (%f)	Cumulative Percentage Frequency (c.%f)
10	3	0.04	3.70	3.70
9	9	0.11	11.11	14.81
8	7	0.09	8.64	23.46
7	8	0.10	9.88	33.33
6	12	0.15	14.81	48.15
5*	8	0.10	9.88	58.02
4	9	0.11	11.11	69.14
3	8	0.10	9.88	79.01
2	5	0.06	6.17	85.19
1	6	0.07	7.41	92.59
0	6	0.07	7.41	100.00
Total	81	1.00	100.00	

**mean (M) and median score*

In Figure 12, the mean (M) and median are equal with eight organizations reporting a preparedness score of 5. In addition, scores span across the index between 10

and zero, with six crisis organizations reporting the lowest score. The greatest number of respondents (12) was reported close the mean (*M*) (5) with a score of six.

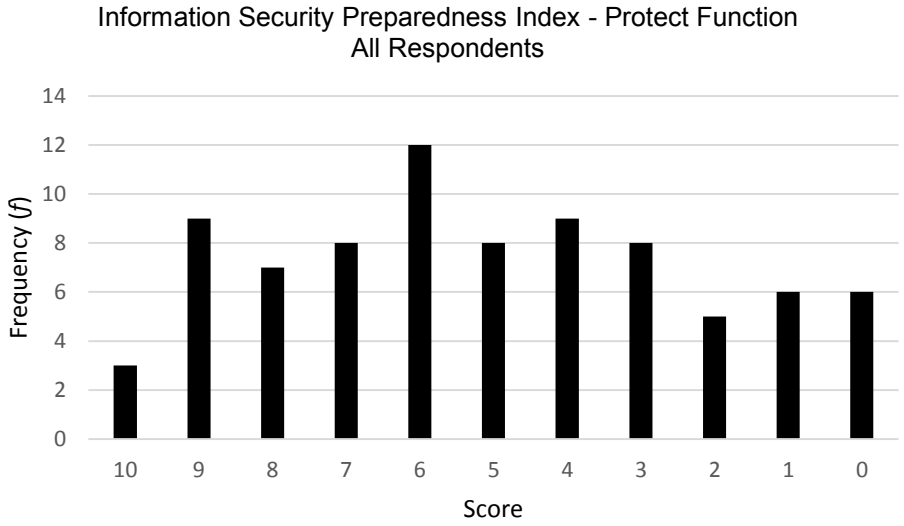


Figure 12. Information security preparedness by the Protect function including crisis organizations servicing victims of domestic violence and human trafficking.

5.3.3.2.3 Domestic Violence not including Human Trafficking

Last, the gap analysis examined the organizations who service domestic violence and not human trafficking against questions mapping to the Protect function. The total number of respondents for this analysis was $n = 70$ and an information security preparedness score of 10. As with the gap analysis conducted for organization services domestic violence and human trafficking victims above, the highest possible score (10) was observed with three respondents with the lowest score (0) reported being four. The number of respondents by preparedness score varied across the sample with 10 respondents scoring a two and nine respondents scoring a nine on the index (see Table 17). The interquartile range similar to the sample of all respondents (Q3 – Q2) of 44.2% was defined between a score of eight and 4.5

Table 17. *Information Security Preparedness Index – Protect Function*

Score	Frequency of Score (*f*)	Relative Frequency (*f/n*)	Percentage Frequency (%*f*)	Cumulative Percentage Frequency (c.%*f*)
10	3	0.04	4.29	4.29
9	9	0.13	12.86	17.14
8	8	0.11	11.43	28.57
7	7	0.10	10.00	38.57
6	4	0.06	5.71	44.29
5*	4	0.06	5.71	50.00
4	8	0.11	11.43	61.43
3	4	0.06	5.71	67.14
2	10	0.14	14.29	81.43
1	9	0.13	12.86	94.29
0	4	0.06	5.71	100.00
Total	70	1.00	100.00	

**mean (M) and median score*

The mean (*M*) and median were both reported at a score of five. However, as illustrated in Figure 13, the greatest number of respondents (10) reported a score of two. Four crisis organizations reported a score of zero.

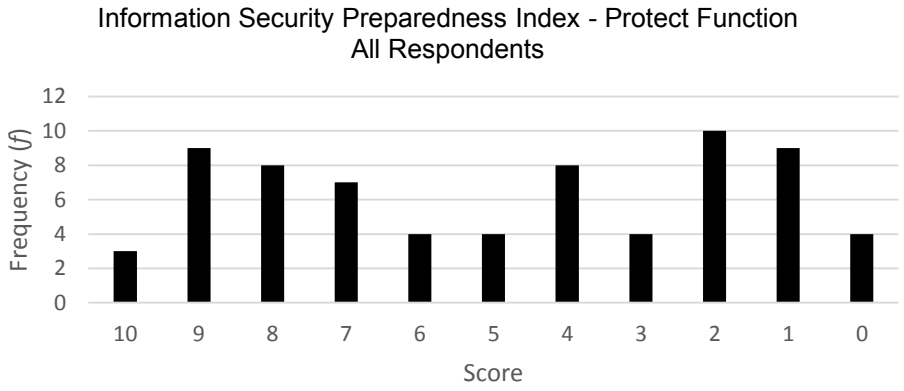


Figure 13. Information security preparedness by the Protect function including crisis organizations servicing victims of domestic violence not including human trafficking.

In conclusion of the frequency analysis for the Protect function, the boxplot diagram in Figure 14 illustrates the upper and lower bounds of the interquartile range for each of the three data sets discussed above. The lower bounds, upper bounds, and mean (*M*) of the all respondents and organizations servicing domestic violence and human trafficking were identical with no outliers were reported.

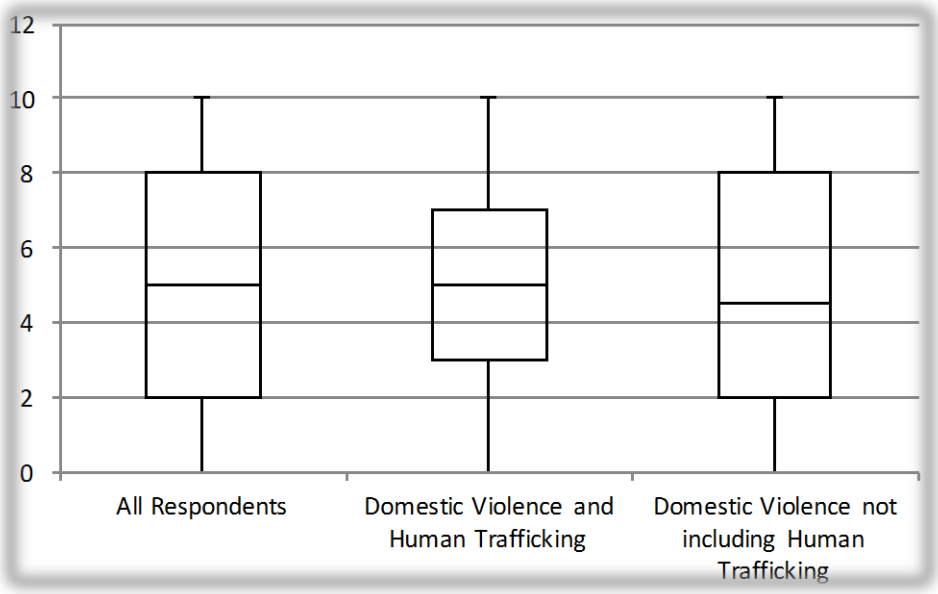


Figure 14. Interquartile range of the information security preparedness index based on the NIST CSF Protect function.

5.3.4 Discussion

For discussion purposes, as a result of the lack of research in this area and inaugural use of the information security preparedness index, organizations who scored above the mean (*M*) in each section below were considered, from an applied perspective, as being within the realm of information security preparedness. A number of organizations across the various areas of analysis scored above the mean (*M*) offering the

potential for continued and applied research in this area to bring more organizations in the ideal state of information security preparedness.

Further analysis on the mean (*M*) was conducted through an independent sample *t*-test to compare the information security preparedness scores of organizations servicing domestic violence and human trafficking, and organizations servicing domestic violence and not human trafficking victims. There was not a significant difference in the scores for organizations servicing domestic violence and human trafficking ($M = 13.7$, $SD = 4.79$), and organizations servicing domestic violence and not human trafficking victims ($M = 12.11$, $SD = 5.38$) conditions; $t\ (149) = 1.902$, $p = .059$. These results suggest that the information security preparedness scores of the category of organizations in this study do not affect each other. However, since the *p* value = .059 is very close to .05, analysis of the data should continue in future research. Refer to Table 17 for detailed results of the *t* test conducted between the information security preparedness scores of organizations servicing victims of domestic violence and human trafficking and organizations servicing domestic violence not including human trafficking victims.

Table 18. *Detailed Results of the t Test*

	Category								
	Domestic Violence and Human Trafficking			Domestic Violence not including Human Trafficking					
	M	*SD*	*n*	*M*	*SD*	*n*	*t*	*df*	*Sig.* (2-tailed)
All Respondents	13.70	4.789	70	12.11	5.385	81	1.902*	149	.0.59

* $p < .05$.

Last, the information security preparedness indices for the six organizations not included in the categories above reported range of scores between 20 and 4. Four out of

the six organizations reported scores above the mean (*M*). These organization service victims of sexual assault, human trafficking, and stalking as reported in the survey. Future research would expand the categories for analysis to include these organizations.

5.4 Exploratory Analysis

The exploratory analysis of this study examined information security preparedness in association with security solutions usage and other pertinent results from survey respondents. There was a positive correlation between the number of technologies organizations reported using and the number of the security technologies they are also using, $r_{pb} = .298$, $n = 158$, $p = .000$. Therefore, as the number of technologies increase within crisis organizations so should the number of security technologies being used. This does not, however, indicate that the security technologies that are being used are appropriate for the risk, a focal point for future research. Refer to Table 19 for the Pearson's Correlation for the number of technologies used by all responding crisis organization with the number of security technologies also used.

Table 19. *Pearson's Correlation for the Number of Technologies Used with the Number of Security Technologies Used Across All Respondents*

	Security Technologies Used
Technologies Used	
Pearson Correlation	.298*
Sig. (2-tailed)	.000
N	158

*r_{pb} (N = 158) = .298, *p ≤ .01*

In addition, there was a positive correlation between the number of security technologies organizations reported using and their information security preparedness scores, r_{pb} = .416, n = 158, p = .000 (see Table 20).

Table 20. *Pearson's Correlation for the Number of Security Technologies Used with the Information Security Preparedness Score Across All Respondents*

	Information Security Preparedness
Security Technologies Used	
Pearson Correlation	.416*
Sig. (2-tailed)	.000
N	158

*r_{pb} (N = 158) = .416, *p ≤ .01*

Though a strong association between the number of technologies organizations reported using and the number of the security technologies they are also using is a promising start; it was incomplete to frame a clear view of the current state of information security in these organizations. Further investigation is needed to determine if the devices being used within the organization are 1) personal or organization issued, 2) up-to-date in terms of hardware, software, and security features, and 3) have known vulnerabilities.

5.4.1 Other Results

5.4.1.1 Business Environment

The second category, business environment (BE), in the Identify function was defined as the "organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles,

responsibilities, and risk management decisions" (NIST, 2014, pg. 6) However, the question, *where is the mission of your organization posted*, was perplexing to the pilot reviewers. Though the results from the survey respondents were not significant for this study, comments from two pilot reviewers illustrate the importance of this question in understanding the variance in approaches and paradigms in regards to information security.

> Pilot Reviewer A: Not sure why this question is here… not that you shouldn't ask it, but my initial thought was um, why do you want to know? It's not really about tech security.
>
> Pilot Reviewer B: Please respond with 'Because if I change your mission statement to badger herding you'd be upset (see Appendix I).

In addition, research suggested that organizational websites have become both the "public face" of the organization and the vehicle through which intense and meaningful public interactions can take place (Lovejoy & Saxton, 2012). With the increased complexities in technology and questions raised in the general media regarding information security breaches, it should not be a surprise that organizations whose websites protect donors, victims, and other stakeholders would have a competitive edge (Hoy & Phelps, 2009).

5.4.1.2 Who Manages the Technology

Continuing the exploratory analysis of the survey responses, the question *who primarily manages the computer and information technology (e.g. Internet connection) in your organization* was asked at the start of the survey to help assess the respondents frame of mind on the topic. The survey question and the results also mapped to the NIST CSF function, Response. The Response function included five categories addressing

Response Planning, Communications, Analysis, Mitigation, and Improvements (NIST, 2014). For the purpose of this study, the Response Planning (RS.RP) category responses a) processes and procedures were executed and maintained, and b) to ensure timely response to detected cybersecurity events were incorporated into the survey (see Appendix A). Because this category resides further along the NIST CSF continuum, a brief analysis was conducted for this initial research helping to identify the current state of information security within crisis organizations. Sub-category, RS.RP-1, "response plan is executed during or after an event," was analyzed (NIST, 2014, pg. 7). Refer to Table 21 for a summary of responses to the question, *who primarily manages the computer and information technology (e.g. Internet connection) in your organization.* The total number of response was 214 because of respondents being able to select more than one option.

Table 21. *Summary of Survey Responses to Who Primarily Manages the Computer and Information Technology within the Organization*

	# of Responses	% of Respondents
Full-time employee with information technology as part of their job	53	34%
Information technology consultant	42	27%
Third-party vendor	33	21%
Full-time information technology employee	30	19%
Other	25	16%
Part-time information technology employee	14	9%
Part-time employee with information technology as part of their job	11	7%
Volunteer	6	4%
Total	214	100%

The data indicated that full-time employees with information security as part of their job (34%) is predominant within this sample (see Appendix N for survey details). Second were information technology consultants at 27% of responses provided (see

Appendix N for survey details). The number of replies for full-time information technology employee was 19% (see Appendix N for survey details). Respondents also offered additional content when responding to "Other" including: "IT company volunteers," "nobody manages it," "Full-time employee with little knowledge not part of the job," "Staff who happen to be knowledgeable (kinda) in IT," "Intern," and "Full-time employee with no information technology as part of their job" (see Appendix N for survey details). These fill-in responses provided additional insight as to where information security, as a priority, falls within the resource management of their organizations.

5.4.1.3 Access to Information Security Resources and Experts

During the 2014 and 2015 NNEDV Tech Summits, the author observed the need and desire by crisis organizations to understand and learn about information security. As a result, questions asking survey respondents if they need more help understanding technology and information security and if they have resources to assist with information security issues were included. The objective was to observe and document respondents perceived need in this area. Results showed that 60% of the sample ($N = 158$) reported wanting more help understand technology and information security with 64% also reporting that they have access to external resources and experts to help with information security. Therefore, the gap that exists is in understanding how, when, and where organizations use their external resources and why they feel they need more help understanding information security. Refer to Table 22 and Table 23 for a summary of survey responses.

Table 22. *Summary of survey responses to if crisis organizations feel they need more help understanding technology and information security.*

	# of Responses	% of Respondents
Yes	95	60%
No	36	23%
Do Not Know	27	17%
Total	158	100%

Table 23. *Summary of survey responses to if crisis organizations have access to external resources and experts to assist with information security.*

	# of Responses	% of Respondents
Yes	91	64%
No	23	16%
Do Not Know	29	20%
Total	158	100%

5.4.1.4 Budget versus Barriers

A 2007 study by Carey-Smith, Nelson, and May from Queensland University of Technology reported that "non-profit organizations and small to medium enterprises have many similarities, the major one being lack of resources" (pg. 39) Therefore, it is possible to conclude that the smaller the organization the less funding they have to put into information security (Carey-Smith, Nelson, & May, 2007). Funding relationships to improve information security within crisis organizations was a key component of the initial vision for this study and corresponds with the research objectives outlined in Chapter 1. Exploring and identifying the gaps between annual budget of crisis organizations and barriers to improving information security were included in this analysis. Refer to Table 24 for a summary of survey responses regarding the barriers to improving information security within crisis organizations.

Table 24. *Summary of Survey Responses to the Barriers to Improving Information Security within Crisis Organizations*

	# of Responses	% of Respondents
Lack of funding	110	70%
Lack of resources (e.g. staff, equipment)	92	58%
Lack of knowledge or understanding of technology	81	51%
Lack of time	76	48%
Focus on other priorities	63	40%
Resistance by staff or other stakeholders	21	13%
Other	11	7%
Do Not Know	9	6%
No Need	7	4%
Total	158	100%

Respondents who selected "Other" provided additional responses relevant for this study, which are listed as follows:

1. "Lack of quality NM trainers"
2. "Part of a larger org that has different standards for other non-victims' services programs and lag behind in understanding our unique needs"
3. "I am a branch within a Tribal Nations full computer system, so they don't understand the need for extreme privacy"
4. "If there is a need I am not aware...that is why we hire IT professional consultants."
5. "Slow Broadband connection"
6. "Budget cuts, expensive internet"
7. "Understanding by IT professionals about our confidentiality requirements"
8. "The City's IT department"
9. "Out dated operating systems"

10. "Addressing confidentiality issues with data storage; finding a software database program to gather required data for funders that doesn't cost $30,000 a year in user fees and maintains support" (see Appendix N for response details).

The top barriers for improving information security with crisis organizations as reported by respondents are:

1. Lack of Funding – 70% of respondents reported
2. Lack of resources (e.g. staff, equipment) – 58% of respondents reported
3. Lack of knowledge or understanding of technology – 51% of respondents reported.

Refer to Table 25 detailing then number of responses by barrier to improving information security.

Table 25. *Summary of Barriers to Improving Information Security*

	# of Responses	% of Respondents
Lack of funding	110	70%
Lack of resources (e.g. staff, equipment)	92	58%
Lack of knowledge or understanding of technology	81	51%
Lack of time	76	48%
Focus on other priorities	63	40%
Resistance by staff or other stakeholders	21	13%
Other	11	7%
Do Not Know	9	6%
No Need	7	4%
Total	158	100%

In addition, it is important to consider if funding will always be the number one barrier for non-profits to improve information security. The options provide in the survey to report the budget, *what is the total annual budget of your organization*, ranged from less than $75,000 to greater than $5,000,000. For this exploratory analysis, a simple

divide at the $500,000 mark was set to observed responses to the barriers for improving information security. Respondents with budgets less than $500,000 reported lack of funding as the primary reason for not being able to improve information security. Also reported within this subgroup was lack of resources and other priorities as the next reasons below lack of funding. Concurrent, respondents with budgets greater than $500,000 also reported of funding as their primary barrier to improving information security with the lack of resources coming in second. Table 26 illustrates the number of responses by subgroup with the barriers to improving information security.

Table 26. *Summary of Barriers to Improving Information Security with Budgets*

Barriers to improving information security?	Respondents with Budgets less than $500,000	Respondents with budgets greater than $500,000
Lack of Funding	32 out of 43 (74%)	59 out of 89 (66%)
Lack of Time	23 out of 43	44 out of 89
Lack of Knowledge	18 out of 43	52 out of 89
Lack of Resources	24 out of 43 (55%)	54 out of 89 (60%)
Other Priorities	24 out of 43 (55%)	36 out of 89
Resistance by Staff	7 out of 43	14 out of 89
No Need	3 out of 43	4 out of 89

5.4.1.5 Attack Knowledge and Preparation

As addressed in Chapter 1, though information security intrusions or attacks on crisis organizations have not been spotlighted in the media does not mean they have not or will not occur. Therefore, the results pertaining to knowledge and preparation for a cyber security attack proved interesting. Looking across the two out of the four questions relevant to cyber attacks was interesting to see 36% don't know if they have identified areas at risk for attack, 60.0% said they have not experienced an attack, 51.0% said they don't know if they are prepared for an attack, and last, 49.0% have not conducted information security workshops or training, all which suggests the important intersections

of awareness, preparedness, and training (see Appendix N for response details). The most striking, yet not surprising, evidence suggested that 78.6% who did not experience a cyber security attack or breach also did not consider themselves prepared to handle an attack or breach if one were to occur. Also, 45.2% of the organizations who didn't know if they had experienced a cyber security attack or breach also do not know if they were prepared (see Appendix N for response details). In addition, 91.1% of organizations who responded "Yes" to having policies for physical security also answered "Yes" to having policies for information security (see Appendix Y for response details).

CHAPTER 6. FUTURE WORK AND CONCLUSIONS

Organizations working with victims of violence are at risk for intrusion and attack every day. Information security researchers and security experts have overlooked non-profit organizations committed to the mission victims of domestic violence, human trafficking, and stalking long enough. This exploratory study achieved the defined research objective to identify the current state of information security within a subset United States based non-profit crisis organizations. Chapter 5 detailed the gaps between a theoretical maximum level of information security and the observed level of information security in the organizations participating in the study. These gaps indicated that information security is evident within crisis organizations, however, below and ideal state of preparedness. The study measured the gaps by looking at information security preparedness using three functions of best practices from the NIST CSF. The gap analysis indicated that preparedness across responses in the Protect function were different then responses in the Identify function. Last, the study documented characteristics of crisis organizations associated with the gap and necessary for ongoing research. The gaps identified throughout the study require future research and investigation to further the body of knowledge in this area and to help crisis organizations improve their state of information security.

The author's experience in this research process, engagement with the domestic violence, stalking, and human trafficking crisis organizations, and ongoing conversations with experts in the security field continue to raise questions and opportunities to narrow the gap between standards that have been established for industry and the unique environment of crisis organizations. Also, as these organizations are growing their online presence and services to clients, it is critical to think proactively through possible attacker profiles, attack vectors, and monitoring systems. Building a culture of security will make the organization more defensible and able to assure clients and stakeholders that increase confidentiality, informed consent, and safety planning. One survey respondent said it well, "These questions are helpful for my own personal awareness; I need to seek more information in these areas. Thank you!"

Basic awareness of how technology works and the risks involved is imperative to safeguarding survivors' personal information, ensuring survivor safety, and holding offenders accountable. Researchers, advocates, and security professionals need to continue to work to help educated crisis organizations change the paradigms around digital security. As it has been said in another context, it is not about waiting for an information security attack or breach to occur in a crisis organization—it is a matter of when. However, the immediacy of the clients' needs takes precedence over internal operations. Creating systems of education, awareness, and training to assist these organizations in improving their internal security infrastructures will have a long term impact. Also, developing assessment tools to continue to understand the state of information security in crisis organization concurrent with creating strategic initiatives will, without a doubt, improve information security for crisis organizations and the

victims they serve. Last, an information security breach in an environment that is built on trust can impact far more than just the data or the services compromised—now is not the time to step back, but step forward with research and action.

6.1 Future Work

As was both hoped and expected, results from the research objectives for this study have raised several areas for continued research that would serve the crisis organizations as defined in this study and other non-profit organizations, other organizations working with victims of violence, and victims and survivors. Several opportunities for future research and development emerged. Below is a brief outline of the top priorities that emerged from the results of this study.

6.1.1 Assessment Tool for Crisis Organizations

Crisis organizations do not need a new framework but an assessment tool that helps to reduce real or imagined fear regarding information security. They need a tool that is written in a language that promotes engagement and thought. As discussed in the previous chapters, the NIST CSF maps to other industry respected assessment tools for information security including COBIT 5 and ISO standards. As the report from Tenable Network Security reveals, "70% of organizations view NIST's framework as a security best practice," however, 83% still report that they will adopt the framework just not in its entirety (Dark Reading, 2016, para. 3).

Implementing the parts of the NIST framework that best suit the environment, as was done with this study, helps to make use of the best practices without the barrier of a high investment. This concept can be carried forward into future efforts to build an assessment tool adapted for crisis organizations and non-profit organizations. An

assessment tool that is based on national standards, yet designed in a language and methodology that helps crisis organizations improve their information security and gain confidence to ask questions and seek help when needed is now possible. Also, now that gaps between the ideal and current state of information security has been identified, core functions that were not included, Detect and Recovery, along with COBIT 5 and the ISO standard can be evaluated to underpin future research in this area.

6.1.2 Expanding Gap Analysis Research

Observing the results of the gap analysis conducted for this study highlighted opportunities for continued work in this area. For example, though two organizations reported no gap between their current and the ideal state of information security preparedness, questions regarding the validity of their responses were raised. As a result, future work could include mechanisms to measure respondents or participating crisis organization understanding of information security language, concepts, and terminology. In addition, establishing methodologies to deeper examine the data to determine if crisis organizations are as far ahead in information security as they reported would provide a more accurate assessment of the current state across the industry. Next, continued efforts and conversations with crisis organizations in relationship to information security best practices offers the possibility to expand the survey and research efforts to include more functions within the NIST CSF; in particular, for those organizations that reported a score on the information security preparedness index.

6.1.3 Characteristics of Crisis Organizations

This study has identified, for the first time, core characteristics of crisis organizations in relationship to information security, including security preparedness as

associated with information security solutions usage. By documenting funding, lack of resources, resource dynamics, and other factors associated information security, the process of understanding the environments in which these organizations function has been started. However, further investigation into the correlations of these characteristics to best practices in information security is needed. This research could be expanded to the larger non-profit sector if the unique characteristics of crisis organizations does not fall too far from sight.

6.1.4 Gaps in Awareness and Training Processes

As revealed in the research and data for this study, awareness, education, and training are critical to the success of any efforts toward improving information security. By arming crisis organizations with comprehensive and customized awareness and education, these organizations will be armed with the confidence they need to ask questions of security experts and make even small incremental improvements. There are some simple steps that may start to raise awareness and set the foundation for training and further work to improve information security within the organization:

1. Get “buy-in” across the organization including directors, staff, volunteers, and other stakeholders that information security should be addressed;
2. Create cross-functional teams including external resources such as legal, victim services, human resources, etc.;
3. Asses the current environment not as a one-time event, but an ongoing process at a frequency that fits the environment;
4. Design awareness, training, and assessment programs that involve staff, victims, and stakeholders.

Areas identified in this study where education could include non-technical users within crisis organization on remote management features included anti-malware solutions, browser and application protections, lock and erase functions, password management, device and software maintenance, and procedures to follow when anomalies are detected.

6.1.5 Strategic Planning Ongoing

Though the development of assessment tools and processes for awareness and training are the recommended top priorities for future research, creating a process to help crisis organizations build strategic plans incorporating information security is critical. The following are elements to begin that process.

1. Technology Solutions. As reported, crisis organizations are making use of several different technologies for a variety of purposes, future research would dive deeper into identifying what technologies are accessible, usable, and contain the appropriate technical capabilities for support or compromising privacy and information security the environment. Areas such as HTTPS, tracking technologies, or spyware should take priority. However, as stated above, before choices in technology are considered, crisis organizations must understand what the choices are and if they are at risk by using technologies with known flaws and vulnerabilities.
2. Foster Ongoing Conversations without Fear. As indicated in Chapter 5, there is a significant gap in understanding how, when, and where organizations use their external resources and why they feel they need more help understanding their vulnerabilities. Designing a strategic approach to information security

policy and procedure could guide crisis organizations to embrace the concept that just because a cyber attack has not happened does not mean that one won't.

3. Identify Key Characteristics. Research must continue in order to understand the unique environment of crisis organizations. This study begins to outline some unique characteristics. However, more work needs to be done that researches how political and cultural obstacles impact information security. As stated by a survey respondent, "Addressing confidentiality issues with data storage; finding a database software program to gather required data for funders that don't (sic) cost $30,000 a year in user fees and maintains support."
4. Ongoing Survey and Research. Further research through the lens of crisis organizations and small non-profits is needed, such as BYOD, attacker profiles, cloud services, and data security. Also, as stated throughout this study, several survey questions need to be analyzed further. It would be helpful to create an improved repeatable survey based on the one used in this study; however, enhanced with a scoring feature would provide researchers with a way to measure improvements (or not) in information security within this domain over time.
5. Maintain a Holistic View. Technology cannot be the only focus by researchers and security experts when addressing the information security of crisis organizations and others. The NIST framework was pivotal to help illustrate the important intersections of people, process, technology, and policy and the

co-dependencies of these variables on the success and security. Without a holistic view, the entire system fails.

6.2 Final Thoughts

This study has set a critical foundation for future research by using a gap analysis to document the current state of information security in organizations working with victims of violence. Using the NIST CSF provided a roadmap that gave this study a foundational place to begin. Now complete, researchers, security experts, and crisis organizations can work together to address the areas of future work, particularly the development of an assessment tool for crisis organizations. Crisis organizations, as evident by conversations with representatives during this study, are ready to learn, to adopt, and to embrace the challenges of understanding information security.

Working to improve information security within crisis organizations is not about transforming crisis organization into experts or pillars of information security. This and future research is intended to raise the bar in awareness and confidence. As seen through the results of the study, staff, victims, and other stakeholders in the crisis organization ecosystem use technology every day without a real understanding of the potential for unintended consequences to actions and the risks to the organization. As technology advances and mobile devices continue to keep people, data, and systems connected, it is without question that crisis organizations need to find ways to assess, anticipate, and minimize the potential for harm to victims, staff, and other stakeholders by securing confidential communications and data collection, storage, and sharing, thereby arming them with the knowledge to ask for help.

This research is one step in a long journey to improve the state of information security in organizations dedicated to helping victims of violence. There are opportunities to expand the body of knowledge in this area even further by learning from crisis organizations and expanding to other non-profit sectors. This research opens the platform for discourse and ideas in a different context to continue the conversation for research and application for crisis organizations and other non-profit organizations. This study accomplished the goal of identifying the current state of information security within crisis organizations while starting the process of prioritizing actionable next steps.

REFERENCES

REFERENCES

A21 Campaign. (n.d.). Abolishing Injustice in the 21st Century. Retrieved from http://www.a21.org/content/terms-conditions/gkrimw?permcode=gkrimw

ANDVSA: Domestic Violence & Sexual Assault Issues in Alaska. (n.d.). Retrieved from http://www.andvsa.org/

Arizona League to End Regional Trafficking. (n.d.). Retrieved from http://www.traffickingaz.org.

Armando, A., Costa, G., & Merlo, A. (2013). *Bring your own device, securely.* Paper presented at the Proceedings of the 28th Annual ACM Symposium on Applied Computing, USA, 1852-1858. doi: 10.1145/2480362.2480707

Atkinson, R., & Flint, J. (2001). Accessing hidden and hard-to-reach populations: Snowball research strategies. *Social Research Update*, *33*(1), 1-4. Retrieved from https://www.researchgate.net/publication/46214232_Accessing_Hidden_and_Hard-to-Reach_Populations_Snowball_Research_Strategies

Atlas Vault. (n.d.). The NIST Cyber-Security Framework and the Importance of 'Identify'. Retrieved from http://www.atlasvault.com/blog/2016/2/29/the-nist-cyber-security-framework-and-the-importance-of-identify.

Banach, M., & Bernat, F. P. (2000). Liability and the internet: Risks and recommendations for social work practice. *Journal of Technology in Human Services*, *17*(2-3), 153-171. doi: 10.1300/J017v17n02_04

Baughman, L. L. (2010). Internet expression in the 21st century: Where technology and law collide: Friend request or foe? Confirming the misuse of internet and social network sites by domestic violence. *Widener Law Journal, 19*(3), 933-977. Retrieved from http://www.victimsofcrime.org/docs/Information%20Clearinghouse/friend-request-or-foe-confirming-the-misuse-of-internet-and-social-networking-sites-by-domestic-violence-perpetrators.pdf?sfvrsn=4

Biswas, C. (2015, March 26). Security for non-profit organizations: 10 tips to help those who help others [Web log post]. Retrieved from https://www.alienvault.com/blogs/security-essentials/security-for-non-profit-organizations-helping-those-who-help-others.

California Against Slavery. (n.d.). Retrieved from http://californiaagainstslavery.org.

Cantwell, J. (2007). New technology means new dangers for domestic violence victims. *AALL Spectrum*, *12*(November), 6-9. Retrieved from http://www.aallnet.org/mm/Publications/spectrum/archives/Vol-12/pub_sp0711/pub-sp0711-prodev.pdf

Carey-Smith, M. T., Nelson, K. J., & May, L. J. (2007). Improving information security management in nonprofit organisations with action research. Paper presented at the Proceedings of the 5th Australian Information Security Management Conference, Perth, Australia. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1023&context=ism

Casa Myrna | Welcome. (n.d.). Retrieved from http://www.casamyrna.org

Centers for Disease Control and Prevention. (2015). Violence prevention. Retrieved from https://www.cdc.gov/violenceprevention/nisvs/.

Cieslak, N. (March 29, 2016*).* NIST cybersecurity framework adoption on the rise. Tenable Network Security [Web log post]. Retrieved from http://www.tenable.com/blog/nist-cybersecurity-framework-adoption-on-the-rise.

Citrix. (2015). Mobile Analytics Report.

Mindlin, J., & Reeves, L. J. H. (2005). Confidentiality and sexual violence survivors: A toolkit for state coalitions. The National Crime Victim Institution at Lewis and Clark Law School. Retrieved from https://law.lclark.edu/live/files/6471-confidentiality-and-sexual-violence-survivors-a.

Corrigan, K. (2001). Putting the brakes on the global trafficking of women for the sex trade: An analysis of existing regulatory schemes to stop the flow of traffic. *Fordham International Law Journal*, *25*, 151. Retrieved from http://ir.lawnet.fordham.edu/ilj/vol25/iss1/6

CyberAngels. (n.d.). Retrieved from http://www.cyberangels.org

Dark Reading. (2016, March 20). NIST cybersecurity framework adoption hampered by costs, survey finds. Dark Reading [Web log post]. Retrieved http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901.

Deflin, B. (2015, July 27). The four fundamentals of cybersecurity. Association for Financial Professionals. Retrieved from http://www.afponline.org/pub/res/news/The_Four_Fundamentals_of_Cybersecurity.html

Elizabeth Stone House. (n.d.). Retrieved from http://www.elizabethstonehouse.org

Federal Trade Commission. (May, 2000). Privacy online: Fair information practices in the electronic marketplace. Retrieved from https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

Finex House: A Massachusetts shelter for battered women and their children. (n.d.). Retrieved from http://finexhouse.org.

Finn, J. (1996). Computer-based self-help groups: A new resource to supplement support groups. *Social Work with Groups, 18*(1), 109-117. doi:10.1300/J009v18n01_11

Finn, J., & Banach, M. (2000). Victimization online: The downside of seeking human services for women on the Internet. *CyberPsychology & Behavior, 3*(5), 785-796. doi:10.1089/10949310050191764

Green, R. (2010). Privacy and domestic violence in court. *William & Mary Journal of Women & Law*, *16*, 237. Retrieved from http://scholarship.law.wm.edu/wmjowl/vol16/iss2/2

HarborCOV. (n.d.). Retrieved from http://harborcov.org

Hoy, M. G., & Phelps, J. (2009). Online privacy and security practices of the 100 largest US nonprofit organizations. *International Journal of Nonprofit and Voluntary Sector Marketing, 14*(1), 71-82.

Hsu, C. C., & Sandford, B. A. (2007). The Delphi technique: making sense of consensus. *Practical Assessment, Research & Evaluation*, *12*(10), 1-8.

International Organization for Standardization (ISO). (n.d.) Retrieved from http://www.iso.org/iso/home.html

ISO Management System Standards. (n.d.). Retrieved from http://www.iso.org/iso/home/standards/management-standards/mss-list.htm

ISO/IEC 27001. (n.d.). Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Intimate Partner Violence. (2015, January 14). Violence prevention. Center for Disease Control and Prevention. Retrieved from http://www.cdc.gov/violenceprevention/nisvs/infographic.html

ISACA. (2012). 5 Essential facts about COBIT. Retrieved from https://www.isaca.org/COBIT/Documents/5-Essential-Facts-about-COBIT.pdf

ISACA. (2014). COBIT online. Retrieved from https://COBITonline.isaca.org

Kirk, J. (2014, November). Rights groups, NGOs struggle against malware attacks. *ComputerWorld*. Retrieved from http://www.computerworld.com/article/2846086/rights-groups-ngos-struggle-against-malware-attacks.html

Kolb, N., & Abdullah, F. (2009). Developing an information security awareness program for a non-profit organization. *International Management Review, 5*(2), 105-110.

Kranz, A. (2002). Changing practice: How domestic violence advocates use internet and wireless communication technologies. MINCAVA electronic clearinghouse. Retrieved from http://www.mincava.umn.edu/documents/2casestudies/2casestudies.pdf

Lovejoy, K., & Saxton, G. D. (2012). Information, community, and action: how nonprofit organizations use social media. *Journal of Computer-Mediated Communication*, *17*(3), 337-353. Retrieved from http://ssrn.com/abstract=2039815

Leach, A. (2014, August). 13 ways to protect your NGO from hacking and surveillance. *The Guardian*. Retrieved from http://www.theguardian.com/global-development-professionals-network/2014/aug/05/hacking-surrveillance-ngo-protect-online-security

McGregor, J. (2014, July). The top 5 most brutal cyber attacks of 2014 so far. *Forbes*. Retrieved from http://www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far/

National Center for Charitable Statistics. (n.d.). US non-profit organizations 2015. Retrieved from http://nccs.urban.org/statistics/upload/US_Nonprofit_Numbers-2.pdf

National Human Trafficking Resource Center. (n.d.). Retrieved from http://traffickingresourcecenter.org

National Institute of Standards and Technology (NIST). (2014, February). Framework for improving critical infrastructure cybersecurity. NIST. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Network to End Domestic Violence. (n.d.). Retrieved from http://nnedv.org

National Network to End Domestic Violence. (n.d.) A glimpse from the field: How abusers are misusing technology [Web log post]. Retrieved from http://techsafety.org/blog/2015/2/17/a-glimpse-from-the-field-how-abusers-are-misusing-technology

National Network to End Domestic Violence. (n.d.) Agency's use of technology best practices and policies toolkit. Retrieved from http://techsafety.org/resources-agencyuse

National Network to End Domestic Violence. (2012). Safety net's technology survey. Retrieved from https://www.surveymonkey.com/r/NNEDVtechnologysurvey

National Network to End Domestic Violence. (2014) New survey: Technology abuse and experiences of survivors and victim services agencies [Web log post]. Retrieved from http://techsafety.org/blog/2014/4/29/new-survey-technology-abuse-experiences-of-survivors-and-victim-services

Needleman, T. (2001, February). A sense of security: Passwords provide a shield. *The Non-profit Times.* Retrieved from http://www.thefreelibrary.com/A+Sense+Of+Security.-a079351950

New York State Coalition Against Domestic Violence. (n.d.). Retrieved from http://www.nyscadv.org

Not for Sale | Working to End Slavery and Human Trafficking. (n.d.). Retrieved from http://notforsalecampaign.org

Petel, J. (2004, April). Information security for churches and small non-profit organizations. Retrieved from https://www.sans.org/reading-room/whitepapers/basics/information-security-churches-small-non-profit-organizations-1373

Peterson, A. (2015, March 20). 2015 is already the year of the health-care hack—and it's only going to get worse. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/

Pfeifle, S. (2015, May). The regulators' view of the Singapore privacy law [Web log post]. Retrieved from https://privacyassociation.org/news/a/the-regulators-view-of-the-singapore-privacy-law/

Ponemon Institute. (2015). 2015 State of the endpoint whitepaper. Lumension. Retrieved from https://www.lumension.com/Lumension/media/graphics/Resources/2015-state-of-the-endpoint/2015-State-of-the-Endpoint-Whitepaper-Lumension.pdf.

Ponemon Institute. (2016). How much is the data in your mobile device worth? Lumension. Retrieved from http://www.ponemon.org/library/how-much-is-the-data-on-your-mobile-device-worth.

Reach Ma. (n.d.). Building healthy communities by ending domestic violence. Retrieved from http://reachma.org/

Renewal House. (n.d.). Retrieved from http://www.uuum.org/?page_id=199

Respond! (n.d.). Retrieved from http://respondinc.org

Rezgui, A., Bouguettaya, A., & Eltoweissy, M. Y. (2003). Privacy on the web: Facts, challenges, and solutions. *IEEE Security & Privacy*, (6), 40-49. Retrieved from http://www.csun.edu/~deb53351/Papers/Rezgui_Privacy_on_the_web.pdf

Sargeant, A., & Lee, S. (2002). Improving public trust in the voluntary sector: An empirical analysis. *International Journal of Nonprofit and Voluntary Sector Marketing*, *7*(1), 68-83. doi:10.1002/nvsm.168

Shahani, A. (2014, September 14). Smartphones are used to stalk, control domestic abuse victims [Web log post]. Retrieved from http://www.npr.org/blogs/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York, NY: NYU Press.

Snijders, T. A. B. (1992). Estimation on the basis of snowball samples: How to weight. *Bulletin de Methodologie Sociologique*, *36*, 59-70. Retrieved from http://www.stats.ox.ac.uk/~snijders/Snijders_BMS1992.pdf

Stalking Resource Center. (n.d.). Retrieved from https://www.victimsofcrime.org/our-programs/stalking-resource-center

Spreen, M. (1992) Rare populations, hidden populations and link-tracing designs: What and why? *Bulletin Methodologie Sociologique*, *36*, 34-58. doi:10.1177/075910639203600103

The History of ISO 17799 and ISO 27001. (n.d.). Retrieved from http://www.pc-history.org/17799.htm

Thomson, S. (1997). *Adaptive sampling in behavioral surveys* (NIDA Research Monograph, Pennsylvania State University). Retrieved from https://archives.drugabuse.gov/pdf/monographs/monograph167/monograph167.pdf#page=301

Tokuyoshi, B. (2013). The security implications of BYOD. *Network Security, 2013*(4), 12-13. doi:10.1016/S1353-4858(13)70050-3

Transition House. (n.d.). Retrieved from http://www.transitionhouse.org

University of Southern California. (2011). Future action for trafficking online. Technology and Human Trafficking. Retrieved from http://technologyandtrafficking.usc.edu/report/future-action-for-trafficking-online/

U.S. Bureau of Justice. (n.d.). Domestic violence cases. Retrieved from http://www.bjs.gov/index.cfm?ty=tp&tid=235

Waldron, V. R., Lavitt, M., & Kelley, D. (2000). The nature and prevention of harm in technology-mediated self-help settings: Three exemplars. *Journal of Technology in Human Services*, *17*(2/3), 267-293. doi:10.1300/J017v17n02_09

Weedon, J. (2014). NGOs: Fighting human rights violations, and now, cyber threat groups [Web log post]. Retrieved from https://www.fireeye.com/blog/threat-research/2014/04/ngos-fighting-human-rights-violations-and-now-cyber-threat-groups.html

Wired Safety. (n.d.). Retrieved from https://www.wiredsafety.org.

Working to Halt Online Abuse. (n.d.). Retrieved from http://www.haltabuse.org

Xia, F., Yang, L.T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems, 25*(9), 1101. doi:10.1002/dac.2417

Zhang, W., Gutierrez, O., Mathieson, K., & Wei, Z. (2010). Information systems research in the nonprofit context: Challenges and opportunities. *Communications of the Association for Information Systems, 27*(1), 1-12. Retrieved from http://aisel.aisnet.org/cais/vol27/iss1/1

Zorza, J. (1995). Recognizing and protecting the privacy and confidentiality needs of battered women. *Family Law Quarterly*, *29*(2), 273-311. Retrieved from http://www.jstor.org/stable/25740031

APPENDICES

Appendix A: NIST Cybersecurity Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	**CCS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CCS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**CCS CSC** 1 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**COBIT 5** APO02.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**COBIT 5** APO03.03, APO03.04, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**COBIT 5** APO01.02, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The	**ID.BE-1:** The organization's role in the supply chain is	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05

	organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	identified and communicated	**ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	**COBIT 5** APO01.03, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4** -1 controls from all families
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	**COBIT 5** APO13.12 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 **NIST SP 800-53 Rev. 4** PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	**COBIT 5** MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1 **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)
		ID.GV-4: Governance and risk management processes address	**COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11,

		cybersecurity risks	4.3.2.4.3, 4.3.2.6.3 **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CCS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	**ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
		ID.RA-3: Threats, both internal and external, are identified and documented	**COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	**COBIT 5** APO12.05, APO13.02 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	**COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **NIST SP 800-53 Rev. 4** PM-9

	decisions.	**ID.RM-3**: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	**NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	**CCS CSC** 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	**COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	**CCS CSC** 12, 15 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	**ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4,

			SC-7
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	**CCS CSC** 9 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2 **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	**CCS CSC** 9 **COBIT 5** APO07.02, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	**CCS CSC** 9 **COBIT 5** APO07.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	**CCS CSC** 9 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	**CCS CSC** 9 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, **NIST SP 800-53 Rev. 4** AT-3, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality,	**PR.DS-1:** Data-at-rest is protected	**CCS CSC** 17 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** SC-28
		PR.DS-2: Data-in-	**CCS CSC** 17

	integrity, and availability of information.	transit is protected	**COBIT 5** APO01.06, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	**COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	**COBIT 5** APO13.01 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.3.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	**CCS CSC** 17 **COBIT 5** APO01.06 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	**ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	**COBIT 5** BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2
	Information Protection Processes and	**PR.IP-1:** A baseline configuration of information	**CCS CSC** 3, 10 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05

	Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	technology/industrial control systems is created and maintained	**ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	**COBIT 5** APO13.01 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	**COBIT 5** BAI06.01, BAI01.06 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	**COBIT 5** APO13.01 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	**COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6

		PR.IP-7: Protection processes are continuously improved	**COBIT 5** APO11.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	**ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	**COBIT 5** DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2 **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	**ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	**COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	**ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	**COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5 **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	**COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4

	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	**CCS CSC** 14 **COBIT 5** APO11.04 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	**COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 2.3 **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	**COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	**CCS CSC** 7 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):**	**DE.AE-1:** A baseline of network operations	**COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

	Anomalous activity is detected in a timely manner and the potential impact of events is understood.	and expected data flows for users and systems is established and managed	**NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	**ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	**ISA 62443-3-3:2013** SR 6.1 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	**COBIT 5** APO12.06 **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Incident alert thresholds are established	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.2.3.10 **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	**CCS CSC** 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	**ISA 62443-2-1:2009** 4.3.3.3.8 **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	**ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1 **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	**CCS CSC** 5 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NIST SP 800-53 Rev. 4** SI-3

		DE.CM-5: Unauthorized mobile code is detected	**ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1 **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	**COBIT 5** APO07.06 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	**NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	**COBIT 5** BAI03.10 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	**CCS CSC** 5 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	**ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Detection processes are tested	**COBIT 5** APO13.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	**COBIT 5** APO11.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6

			NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	**COBIT 5** BAI01.10 **CCS CSC** 18 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	**ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	**ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	**ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	**ISA 62443-2-1:2009** 4.3.4.5.5 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	**NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	**COBIT 5** DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	**ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.6

			NIST SP 800-53 Rev. 4 CP-2, IR-4
		RS.AN-3: Forensics are performed	**ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	**ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	**ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	**ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	**ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	**NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	**CCS CSC** 8 **COBIT 5** DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8

	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	**COBIT 5** BAI05.07 **ISA 62443-2-1** 4.4.3.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	**COBIT 5** BAI07.08 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	**COBIT 5** EDM03.02
		RC.CO-2: Reputation after an event is repaired	**COBIT 5** MEA03.02
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	**NIST SP 800-53 Rev. 4** CP-2, IR-4

(NIST, 2014)

Appendix B: Crisis Organizations Website Review

The preliminary research conducted for this a study included a review of the websites of 20 crisis organizations and document the social media platforms being used.

Organization	Website	Facebook	Twitter	YouTube	Other
A21 Campaign (A21 Campaign, n.d.)	X	X	X	X	Instagram
Arizona League to End Regional Trafficking (Arizona League to End Regional Trafficking, n.d.)	X	X			
Asian Shelter and Advocacy Project (Shelter Program Improvement Fund, n.d.)	X	X			LinkedIN
California Against Slavery (California Against Slavery, n.d.)	X	X	X	X	
Casa Myrna Vazquez (Casa Myrna, n.d.)	X	X	X	X	
Cyber Angels (CyberAngels, n.d)	X				
Elizabeth Stone House (Elizabeth Stone House, n.d.)	X	X	X		
FINEX House (Finex House, n.d.)	X				
Harbor COV (HarborCOV, n.d.)	X	X	X		Tumblr, Google+
National Human Trafficking Resource Center (National Human Trafficking Resource Center, n.d.)	X				
National Network to End Domestic Violence - including the Safety Net Project (National Network to End Domestic Violence, n.d.)	X	X	X	X	Google+, Flickr, Pinterest
New York State Coalition Against Domestic Violence	X	X	X		

Organization	Website	Facebook	Twitter	YouTube	Other
(New York State Coalition Against Domestic Violence, n.d.)					
Not for Sale (Not For Sale, n.d.)	X				
REACH Beyond Domestic Violence (Reach Ma, n.d.)	X				
Renewal House (Renewal House, n.d.)	X				
Respond (Respond!, n.d.)	X	X	X	X	LinkedIN
Stalking Resource Center (Stalking Resource Center, n.d.)	X	X	X		
Transition House (Transition House, n.d.)	X	X	X		
Wired Safety (Wired Safety, n.d.)	X	X	X	X	
Working to Halt Abuse (Working to Halt Online Abuse, n.d.)	X				

Appendix C: Survey Development

The final survey was developed using both the 2012 NNEDV survey and the NIST CSF (NIST, 2014). Below maps each survey question to the source.

Question	NNEDV	NIST
Q1: Consent Form	n/a	n/a
Q2: What type(s) of victims or survivors does your organization serve?	✓	
Q3: What is the size of your organization?	✓	
Q4: Who primarily manages the computers and information technology (e.g. Internet connection) in your organization?		RS.RP-1
Q5: What is the total annual budget of your organization?	✓	
Q6: Where is the mission of your organization posted?		ID.BE-3
Q7: What technologies does your organization use?	✓	
Q8: What computer operating systems does your organization use?	✓	
Q9: Does your organization currently use any of the following security technologies?	n/a	n/a
Q10: How does your staff access the Internet?	✓	ID.GV-1
Q11: Does your staff access organizational electronic documents from outside the premises?		ID.AM-3 ID.GV-1
Q12: What social media does your organization use?	✓	
Q13: Who in your organization is responsible for	✓	

Question	NNEDV	NIST
managing the organization's social media channel(s)?		
Q14: For what purpose(s) does your organization use social media? (check all that apply)	✓	
Q15: Does your organization have human resources policies regarding social media use by the following?	✓	
Q16: Do you feel you need more help understanding technology and information security?	n/a	n/a
Q17: In general, what type(s) of training are most effective in your organization?	✓	
Q18: What do you perceive are barriers to improving your organization's information security?	✓	
Q19: Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies in belonging to the organization?		ID.AM-1 ID.AM-2 ID.AM-5
Q20: Do you know if these items are insured against theft or loss?		ID.AM-1
Q21: Is the software used by your organization inventoried?		ID.AM-2
Q22: Has your organization identified what hardware and software are critical to your operations?		ID.AM-5
Q23: Does your organization have policies or documented plans for power or Internet outages?		ID.BE-4
Q24 Does your organization have policies for physical security?		ID.BE-4 ID.GV-1

Question	NNEDV	NIST
Q25: Does your organization have policies for information security?		ID.AM-3 ID.BE-4 ID.GV-1 PR.AC-1
Q26: If yes, which technologies do these policies include?		ID.BE-4 ID.GV-1
Q27: Who is responsible for information security within the organization?		ID.AM-6 ID.GV-2
Q28: Who in your organization is responsible for the legal requirements for information security? (e.g. GLBA, HIPPA compliance, protective orders, etc.)		PR.AT-2
Q29: Are the legal requirements listed in Question 28 regarding information security understood by those responsible?		PR.AT-2
Q30: Has your organization identified areas or practices that may be attractive targets or vulnerable for a cyber attack or breach?		ID.RM-1
Q31: Has your organization experienced a cybersecurity attack or breach?		ID.RM-1 RS.RP-1
Q32: Does your organization consider itself prepared to handle a cybersecurity breach or attack?		ID.RM-1
Q33: Has your organization conducted information security workshops or training with staff, volunteers, and other stakeholders?		ID.RM-1 PR.AT-1
Q34: If yes or plan to soon, who will conduct the training?		ID.RM-1
Q35: Does your organization document who has access to sensitive files, databases, and other		PR.AC-1

Question	NNEDV	NIST
electronic information?		
Q36: Does your organization inform or train new employees about information security policies and procedures?		PR.AT-1
Q37: Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures?		ID.AM-6 PR.AT-1
Q38: If your organization does use third-party vendors do they inform you of their information security policies and procedures?		PR.AT-1
Q39: How is access to electronic files containing sensitive information stored within your organization protected?		PR.AC-1
Q40: Does your organization have policies and procedures for the destruction of electronic documents?		PR.IP-6
Q41: Does your organization have policies and procedures for the destruction storage devices? (e.g. DVDs, CDs, thumbdrives, etc.)		PR.IP-6
Q42: Does your organization have access to external resources and experts to help with cyber security?	n/a	n/a
Q43 Please provide any additional information regarding the current state of information security within your organization.	n/a	n/a
Q44 If you would like to receive a statistical summary of this survey at the conclusion of this study, please provide your contact information.	n/a	n/a

(NIST, 2014), (NNEDV, 2012)

Appendix D: IRB Application and Amendment

Institutional Review Board

1. Project Title: Identifying the Current State of Information Security within Crisis Organizations

2. Full Review ☐ Expedited Review X

3. Anticipated Funding Source: None

4. Principal Investigator *[See Policy on Eligibility to serve as a Principal Investigator for Research Involving Human Subjects]*:

   Dr. Eugene Spafford
   Professor of Computer Science
   Lawson Building, Room 1183
   (765) 494-7825
   spaf@purdue.edu

5. Co-investigators and key personnel *[See Education Policy for Conducting Human Subjects Research]*:

   Kelley Kathleen Misata Nybakken
   PhD Candidate
   Lawson Building, Room 1183
   (617) 650-0601
   kmisata@purdue.edu

6. Consultants *[See Education Policy for Conducting Human Subjects Research]*:
   N/A

7. The principal investigator agrees to carry out the proposed project as stated in the application and to promptly report to the Institutional Review Board any proposed changes and/or unanticipated problems involving risks to subjects or others participating in the approved project in accordance with the HRPP Guideline 207 Researcher Responsibilities, Purdue Research Foundation-Purdue University Statement of Principles and the Confidentiality Statement. The principal investigator has received a copy of the Federal-Wide Assurance (FWA) and has access to copies of 45 CFR 46 and the Belmont Report. The principal investigator agrees to inform the Institutional Review Board and complete all necessary reports should the principal investigator terminate University association.

   _____
   Principal Investigator Signature Date

8. The Department Head (or authorized agent) has read and approved the application. S/he affirms that the use of human subjects in this project is relevant to answer the research

question being asked and has scientific or scholarly merit. Additionally s/he agrees to maintain research records in accordance with the IRB's research records retention requirement should the principal investigator terminate association with the University.

_____
_____
Department Head *(printed)* Department Name

_____
_____
Department Head Signature Date

9. This project will be conducted at the following location(s): (please indicate city & state)

☐ Purdue West Lafayette Campus
☐ Purdue Regional Campus (Specify): _____
X Other (Specify): Online - survey participants will review the survey and/or fill-out the evaluation form at his/her place of employment, all of which are located throughout the United States.

10. If this project will involve potentially vulnerable subject populations, please check all that apply.

☐ Minors under age 18
☐ Pregnant Women
☐ Fetus/fetal tissue
☐ Prisoners Or Incarcerated Individuals
☐ University Students (PSYC Dept. subject pool ___)
☐ Elderly Persons
☐ Economically/Educationally Disadvantaged Persons
☐ Mentally/Emotionally/Developmentally Disabled Persons
☐ Minority Groups and/or Non-English Speakers
☐ Intervention(s) that include medical or psychological treatment

11. Indicate the anticipated maximum number of subjects to be enrolled in this protocol as justified by the hypothesis and study procedures: 20 – Pilot Review

12. This project involves the use of an **Investigational New Drug** (IND) or an **Approved Drug For An Unapproved Use**.

☐ YES X NO
Drug name, IND number and company: _____

13. This project involves the use of an **Investigational Medical Device** or an **Approved Medical Device For An Unapproved Use**.

☐ YES X NO
Device name, IDE number and company: _____

14. The project involves the use of **Radiation or Radioisotopes**:

☐ YES X NO

15. Does this project call for: (check-mark all that apply to this study)

☐ Use of Voice, Video, Digital, or Image Recordings?

☐ Subject Compensation? Please indicate the maximum payment amount to subjects.
Purdue's Human Subjects Payment Policy Participant Payment Disclosure Form

☐ VO2 Max Exercise?

☐ More Than Minimal Risk?

☐ Waiver of Informed Consent?

☐ Extra Costs To Subjects?

☐ The Use of Blood? Total Amount of Blood _____
Over Time Period (days) _____

☐ The Use of rDNA or Biohazardous materials?

☐ The Use of Human Tissue or Cell Lines?

☐ The Use of Other Fluids that Could Mask the Presence of Blood (Including Urine and Feces)?

☐ The Use of Protected Health Information (Obtained from Healthcare Practitioners or Institutions)?

☐ The Use of academic records?

16. Does investigator or key personnel have a potential financial or other conflict of interest in this study?

☐ YES X NO

APPLICATION NARRATIVE

A. PROPOSED RESEARCH RATIONALE

- This research is intended to improve the current state of information security within organizations working with victims of violence. The study will identify the intersection of technology, policies, and people in information security as it pertains to the unique environment of crisis organizations against a recognized and respect framework for information security. It will advance the current state of research by establishing an overdue foundation for future research in information security for crisis and other non-profit organizations. The problem this research will address is to establish a much-needed baseline for which crisis organizations to build effective cyber security strategies and improvement initiatives.

B. SPECIFIC PROCEDURES TO BE FOLLOWED

- Pilot Survey Review:
  - 20 subject matter experts will be recruited to review the survey.
  - The pilot survey review will be conducted in two rounds.
  - Round one will commence by sending an email a group of high-level executives with subject matter knowledge who will be

identified by the research team to answer the pilot survey reviewers. The email will include instructions regarding their role and responsibilities as a pilot survey reviewer, a link to the online survey in Qualtrics, and an evaluation sheet attachment in MSWord to record their feedback. These individuals will be identified by authorship of journals, prior identification of expertise in this field (for example).
    - After acknowledging agreement to the consent form, the participant will take the short survey. Participants will fill out the evaluation form during or immediately following their review of the online survey.
    - Participants will send all feedback forms back to the co-investigator for compiling.
    - Once the data compiled, in round two, participants will receive an emailed with the results of round one and an opportunity to provide any additional thoughts or feedback on the survey, based on the responses of the other participants.
    - At the end of the survey and completion of the evaluation forms, the participant's involvement will be complete.
    - The data collected from both rounds will be the final comments and suggestions provided by the participants.
    - The survey will be updated based on the feedback received and submitted to IRB as an amendment to this application.
- General Survey
    - An invitation to participate and a link in the online survey will be sent to the crisis organization from the National Network to End Domestic Violence, Thorn, and Demand Abolition.
    - 700 – 1000 direct service and coordinated crisis organizations will receive the invitation and the online survey link.
    - The respondent from each organization will be considered the participant.
    - At the start of the survey on Qualtrics, each participant will be required to read and agree to an online consent form.
    - After acknowledging agreement to the consent form, the participant will take the short survey.
    - At the end of the survey, the participant's involvement will be complete.
    - The data collected will be the answers provided to the survey questions by the participants.

C. SUBJECTS TO BE INCLUDED

Describe:

- Pilot Survey Review:
    - The inclusion criteria are to be high or executive level people with expertise in crisis organizations, information security, and non-

profit organizations.
    - There will be no special population involvement.
    - The number of participants that are sought to be included is 15 - 20.
- General Survey:
    - The inclusion criteria are to be people employed by direct or coordinated service crisis organizations working with victims of violence identified by the National Network to End Domestic Violence (NNEDV), Thorn, and Demand Abolition.
    - Invitations to participate and the link to the survey will be sent directly to the contacts from the National Network to End Domestic Violence (NNEDV), Thorn, and Demand Abolition.
    - There will be no special population involvement.
    - The number of participants that will be invited to participate is 700 – 1000

D. RECRUITMENT OF SUBJECTS AND OBTAINING INFORMED CONSENT

- Pilot Survey Review:
    - Participants will be recruited based on their expertise in crisis organizations, information security, and non-profit organizations.
    - Participants will be high or executive level decision makers in their organizations; thereby not requiring additional permission to participate as a pilot survey reviewer.
    - Participants will be individually invited via email and phone conversations to participate as a pilot survey reviewer.
    - There will be no special population involvement.
    - The number of participants that are sought to be included is 15 - 20.
- General Survey:
    - Participants will be direct and coordinated service crisis organizations identified by the National Network to End Domestic Violence (NNEDV), Thorn, and Demand Abolition.
    - Invitations to participate and link for the survey will be sent directly to the contacts from the National Network to End Domestic Violence (NNEDV), Thorn, and Demand Abolition.
    - An initial email with survey details and links will be provide to NNEDV, Thorn, and Demand for Abolition for distribution to their contacts.
    - Two reminder emails will be provided to to NNEDV, Thorn, and Demand for Abolition for distribution to their contacts.
    - There will be no special population involvement.
    - The number of participants that will be invited to participate is 700 - 1000.

E. PROCEDURES FOR PAYMENT OF SUBJECTS

- No compensation will be paid to any participating agency.

F. CONFIDENTIALITY

- No personal identifying information will be collected. Also, only individuals previously invited will participate in the study.
- Research records will be stored in .docx (MSWord) or .xls (Excel) format on a dedicated hard drive located at the co-investigators address in Brookline, MA. A de-identified hard-copy of the results will be held on campus at Purdue University. The data will be deleted from Qualtrics when the survey is completed.
- Access will be limited initially to only the principal investigator and key personnel.
- After two years, the principal investigator will determine whether the data should be shared with others outside the study for future research purposes.
- Three years after the initial collection, the principal investigator will determine whether the data should be destroyed.
- There will be a virtual consent form that the participants will be required to review and agree to before completing the survey. They will accept the consent form by clicking on the "I agree" button.

G. POTENTIAL RISKS TO SUBJECTS

- Pilot survey reviewers will be invited to participate, therefore, this research poses minimal risk and no greater than everyday activities.
- The identities of the general survey participants will not be known as the invitation to participate and the online survey link will be sent directly from the NNEDV, Thorn, and Demand Abolition. Therefore, this research poses minimal risk and no greater than everyday activities.
- There is a potential risk to participants of a data breach, which will be minimized by storing all responses and research results on a dedicated hard drive resulting in minimal risk.

H. BENEFITS TO BE GAINED BY THE INDIVIDUAL AND/OR SOCIETY

- There are no direct benefits to the participants involved in this study.
- There are potential benefits to the participants that they may better understand the current state of information security within organizations working with victims of violence.
- The benefits to society are creating a comprehensive survey being used in the next phase of this research in identifying the risks, opportunities, and priorities crisis organizations can address to improve their current state of information security; with the possibility of keeping the survivors they service safer in the process.

I. INVESTIGATOR'S EVALUATION OF THE RISK-BENEFIT RATIO

- The research does not pose greater than minimal risk to participants than everyday activities.
- The benefits of the research outweigh any potential risks.
- There are no direct benefits to the participants but the potential benefits to society in analyzing the gaps in the current state of information security in organizations working with victims of violence against a recognized framework far outweighs the minimal risks.

J. WRITTEN INFORMED CONSENT FORM

- Informed Consent Form is attached to this application.

K. WAIVER OF INFORMED CONSENT OR SIGNED CONSENT

- There is no request for a Waiver of Consent Request for this study.
- This study is requesting a Waiver of Signed Consent.
    - The research does not pose greater than minimal risk to participants than everyday activities.
    - A breach of confidentiality does constitute the principal risk to participants.
    - The signed consent form and email correspondence with the co-investigator would be the only record linking the participant and the research.
    - The research does not include any activities that would require signed consent in a non-research context.
    - The participants will be provided a written statement via email and online through Qualtrics about the research. The consent form will consist of an information sheet that contains all the elements of the consent form but without the signature lines that will require the participant to agree to the terms prior to reviewing any survey questions.

Appendix E: Pilot Reviewers

Name	*Position*	*Pilot Reviewer*
Ed Moyle	Director of Emerging Business and Technology, ISACA	Yes
Tim Casey	Cyber Risk Systems Architect at Intel	
Michael Diamond	Board Member (Secretary) at International Association of Security Awareness Professionals (IASAP) and Training and Awareness Manager of Information Security and Privacy at Intel	Yes
Risa Mednick	Executive Director, Transition House	Yes
Laura Van Zandt	Executive Director, Reach Beyond Domestic Violence	No
Lauren Montanaro	Shelter Coordinator, Reach Beyond Domestic Violence	Yes
Kaofeng Lee	Deputy Director of the Safety Net Project at the National Network to End Domestic Violence	Yes
Cindy Southworth	Executive Vice President National Network to End Domestic Violence	No
Erica Olsen	Technology Safety Specialist for the Safety Net Project	Yes
Ebony Tucker, JD	Executive Director, LaFASA	Yes
Tori Placona	Outreach Coordinator LaFASA	Yes
Leah Treitman	Program Coordinator at We Are Thorn	Yes
Becky Bace	Chief Strategist, Center for Forensics, Information Technology, and Security (CFITS) at University of South Alabama	Yes
Delaney Workman	Demand Abolition Social Innovation Coordinator	No
Dhakir Warren	Demand Abolition Senior Manager	No
Greg Virgin	President and CEO RedJacket	Yes
Diana Kelley	Executive Security Advisor, IBM Security	Yes
Jenny Backus	Senior Policy Officer, Google	No
Stacy Martin	Senior Manager, Privacy and Engagement at Mozilla Corporation	No
Teri Gilbert	Chief Technology Officer, Verdafero, Inc.	No

Appendix F: Pilot Review Evaluation Form

As outlined in the methodology section above, the pilot group reviewed the general survey for clarity, consistency, and ease of use for the organizations identified in this study. The pilot review used the Delphia approach with two rounds of review (Hsu & Sandford, 2007). The evaluation form below was used for only the first round of review. The second round allowed pilot reviews to adjust their comments and suggestions based on a detailed report of the round one results.

Question	No Change Needed	Language Too Technical	Confusing	Does Not Fit Objective	Other*
1. Type of Program					
2. Organization Size					
3. Budget Size					
4. Where is the organization's website posted?					
5. What computer operating system does your organization use?					
6. What types of technology does your organization use?					
7. Does your organization currently use any of the following security products?					
8. Who manages and maintains your technology, computer systems, cyber security?					
9. How does your staff access the Internet?					
10. What social media does your organization use?					
11. Why does your organization use social media?					
12. Who in your organization manages and monitors the organization's social media?					
13. Does your organization have policies and procedures regarding social media use for the following?					
14. Do you feel you need more information regarding technology and cyber security?					
15. What type(s) of training are most effective for your organization?					
16. What are some barriers to improving your					

organization's cyber security and understanding of technology in general?					
17. Are all computers, laptops, cellphones, and other technologies inventoried and documented?					
18. Do you have an inventory of all software applications being used by the organizations?					
19. If yes, do the inventories of both hardware and software prioritize the technology based on criticality or value to the organization?					
20. Does staff within the organization have specific cyber security duties or responsibilities?					
21. Do you have a back-up policy, procedure, and system for power or Internet outages?					
22. Do you have policies regarding cyber security?					
23. Which technologies do these policies include?					
24. Who in you organization is responsible for maintenance and the security of the organization's technology?					
25. Who in your organization is responsible for legal and regulatory requirements for cyber security including privacy rights and civil liberties?					
26. Are the legal and regulatory requirements regarding cyber security understood by those responsible?					
27. Has your organization experienced a cyber security attack or breach?					
28. Has your organization identified areas that may be attractive or vulnerable for cyber attack or breach?					
29. Have you conducted conversations with staff, board members, volunteers, and others regarding cyber security?					
30. Have you documented the identities and credentials of the staff members that access to files, databases, and other electronic information?					
31. Do you inform staff about cyber security policies, practices, and procedures?					
32. Do you inform third-party vendors and partners about cyber security policies, practices, and procedures?					
33. With survivor and other sensitive information stored in digital files, is this information protected by any of the following?					
34. Do you have a policy for the destruction of digital files and information?					

35. Has your organization experienced a cyber security breach or attack?					
36. If yes, was the situation clearly understood by all?					
37. Did you feel or do you feel adequately prepared for a cyber security breach or attack					
38. Do you have access to resources and experts to help your organization with cyber security?					
39. Contact Information (optional)					

1. The survey is intended to take participants 10 minutes or less to complete, do you think the length of the survey and complexity of the questions will meet this objective?
   - Yes
   - No
   - Do Not Know

2. Does the order of the questions make sense?
   - Yes
   - No

   If no, please provide suggestions:

3. If you have suggestions on a specific survey question(s) please provide it below.

4. Please feel free to provide additional comments or suggestions regarding the survey, any feedback is appreciated.

Thank you for filling out this evaluation form. The information you provide is the first step in helping organizations working with victims of violence stay safe in a digital world.

Please be advised, the names and organizations of those participating in this pilot are anonymous, unless otherwise requested. Results from round one of this review will be shared with the group allowing an opportunity to update your comments and feedback in the second round.

If you would like a copy of the final report at the conclusion of this study or have any questions, please contact Kelley Misata (kmisata@purdue.edu).

Appendix G: Pilot Review Round One – Email Script

On December 10, 2015, the members of the pilot group were individually contact to launch the first stage of the survey review process. The following is the email template used for this initial outreach.

Dear [name]:

You are invited to participate in the "pilot" phase of a research study aimed at identifying the current state of information security within organizations working with victims of violence. The goal of the "pilot" review is to gather input from industry experts, such as you, on the survey for crisis organizations in the study. Experts in crisis organizations and information security are being invited to participate in this study.

This review process consists of two rounds:

First, round one... in this round you will be asked to review the survey titled "Information Security in Crisis Organizations" and provide your feedback using the attached evaluation form. You may access the survey either online using the link below OR using the attached survey file. **Time: less than 45 minutes.**

Please return the feedback form via email to me at kmisata@purdue.edu on or before December 20, 2015.

Second, round two... once the results from Round One have been compiled, a complete report will be sent to all pilot group participants. At this time, you will be invited (though not required) to update your feedback from the first round. **Time: approx. 30 minutes.**

To get started:
1. Download the attached evaluation form;
2. Click **https://purdue.qualtrics.com/SE/?SID=SV_d1qdm7N4rZlAGuF** to enter the online survey – note: you will need to click "I Agree" to begin. You are NOT required to fill out the survey to do the evaluation. You may also use the attached survey file;
3. Return the completed evaluation form on or before December 20th.

If you choose to participate your input will be invaluable in helping organizations working with victims of violence to navigate the complexities of cybersecurity. Participation is entirely voluntary, and you can stop participating at any time with no consequences.

Also, if you have questions, please contact me at kmisata@purdue.edu or (617) 650-0601.

Appendix H: Pilot Review Survey

The following survey was used for the pilot group as the initial reviewers prior to the survey being conducted with the larger population outlined in this study. Once feedback is received the survey was updated based on the suggestions provided by the pilot group then re-submitted to the IRB as an amendment for approval. This survey was designed using the National Network to End Domestic Violence survey executed in 2012 and the NIST CSF (NNEDV, 2012) (NIST, 2014).

1. Type of Program (check all that apply)
   - ☐ Domestic Violence
   - ☐ Sexual Assault
   - ☐ Human Trafficking
   - ☐ Stalking
   - ☐ Other (fill-in)

2. Organization Size
   Number of Full-Time Employees: (fill-in)
   Number of Part-Time Employees
   Number of Volunteers: (fill-in)

3. Budget Size
   - o Less than $75,000
   - o $75,000 - $149,000
   - o $150,000 - $349,000
   - o $350,000 - $499,999
   - o $500,000 - $999,999
   - o >$1,000,000
   - o Do Not Know

4. Where is the organization's mission posted? (check all that apply)
   - ☐ Website
   - ☐ Hardcopy Marketing
   - ☐ Social Media
   - ☐ Other (fill-in)

5. What computer operating system does your organization use? (check all that apply)
   - ☐ Apple / Mac OS
   - ☐ Microsoft Windows
   - ☐ Linux
   - ☐ Other (fill-in)

6. What types of technology does your organization use? (check all that apply)
   - ☐ Desktop Computers
   - ☐ Laptops / Notebooks

- ☐ iPad / Tablets
- ☐ iPhones
- ☐ Android Phones
- ☐ Other Cell Phones
- ☐ Land-line Phones
- ☐ Fax Machines
- ☐ Cameras
- ☐ Surveillance Monitoring Cameras
- ☐ Other (fill-in)

7. Does your organization currently use any of the following security products? (check all that apply)
   - ☐ Firewall
   - ☐ Anti-Virus Software
   - ☐ Password Protection
   - ☐ VPNs
   - ☐ Proxy Services
   - ☐ Cloud Storage
   - ☐ Do Not Know

8. Who manages and maintains your technology, computer systems, cyber security?
   - o Dedicated IT Person
   - o Full-Time Employee
   - o Part-Time Employee
   - o Volunteer
   - o IT Consultant
   - o Third-Party Vendor
   - o Do Not know

9. How does your staff access the Internet? (check all that apply)
   - ☐ High-Speed Internet (connected via a wire)
   - ☐ Wireless Internet
   - ☐ Mobile HotSpot
   - ☐ Other (fill-in)
   - ☐ Do Not Know

10. What social media does your organization use? (check all that apply)
    - ☐ Website
    - ☐ Blog
    - ☐ Facebook
    - ☐ Twitter
    - ☐ Instagram
    - ☐ LinkedIN
    - ☐ YouTube
    - ☐ Flickr

- ☐ None
- ☐ Other (fill-in)

11. Why does your organization use social media? (check all that apply)
    - ☐ Awareness
    - ☐ Education
    - ☐ Fundraising
    - ☐ Outreach
    - ☐ No Defined Purpose
    - ☐ Other (fill-in)

12. Who in your organization manages and monitors the organization's social media? (check all that apply)
    - ☐ Dedicated full-time employee
    - ☐ Dedicated part-time employee
    - ☐ Shared responsibility with multiple employees in the organization
    - ☐ Contractor
    - ☐ Volunteer
    - ☐ Third-Party Communications
    - ☐ Do Not Know

13. Does your organization have policies and procedures regarding social media use for the following? (check all that apply)
    - ☐ Staff
    - ☐ Volunteers
    - ☐ Victims / Survivors
    - ☐ Do Not Know
    - ☐ Others (fill-in)

14. Do you feel you need more information regarding technology and cyber security?
    - o Yes
    - o No
    - o Do Not Know

15. What type(s) of training are most effective for your organization? (check all that apply)
    - ☐ In-person Training
    - ☐ Onsite Training
    - ☐ Web-based Training
    - ☐ Hardcopy Materials
    - ☐ Other (fill-in)

16. What are some barriers to improving your organization's cyber security and understanding of technology in general? (check all that apply)
    - ☐ Lack of funding

- ☐ Lack of time
- ☐ Lack of knowledge / understanding of technology
- ☐ Lack of resources
- ☐ Focus on other priorities
- ☐ Resistance by staff or others
- ☐ No need

17. Are all computers, laptops, cellphones, and other technologies inventoried and documented?
    - o All and documented
    - o Some and documented
    - o All but not documented
    - o Some but not documented
    - o None
    - o Do Not Know

18. Do you have an inventory of all software applications being used by the organizations?
    - o Yes
    - o No
    - o Do Not Know

19. If yes, do the inventories of both hardware and software prioritize the technology based on criticality or value to the organization?
    - o Yes
    - o No
    - o Do Not Know

20. Does staff within the organization have specific cybersecurity duties or responsibilities?
    - o Yes
    - o No
    - o Do Not Know

21. Do you have a back-up policy, procedure, and system for power or Internet outages?
    - o Yes
    - o No
    - o Do Not Know

22. Do you have policies regarding cyber security?
    - o Yes
    - o No
    - o Do Not Know

23. Which technologies do these policies include? (check all that apply)

- ☐ Use of laptops and organization issued computers.
- ☐ Use of cellphones issued by the organization.
- ☐ Use of personal cell phones and other technologies.
- ☐ Use of social media for organizational purposes.
- ☐ Use of personal social media in reference to working at the organization.
- ☐ Use of public Wi-Fi
- ☐ Protection of passwords.
- ☐ Others (fill-in)

24. Who in your organization is responsible for maintenance and the security of the organization's technology? (check all that apply)
    - o Executive Director
    - o Manager / Director
    - o Staff Member
    - o Consultant
    - o Volunteer
    - o Third-Party Service Provider
    - o Other (fill-in)

25. Who in your organization is responsible for legal and regulatory requirements for cyber security including privacy rights and civil liberties?
    - o Executive Director
    - o Manager / Director
    - o Staff Member
    - o Consultant
    - o Volunteer
    - o Third-Party Legal Service Provider
    - o Other (fill-in)

26. Are the legal and regulatory requirements regarding cyber security understood by those responsible?
    - o Yes
    - o No
    - o Do Not Know

27. Has your organization experienced a cybersecurity attack or breach?
    - o Yes
    - o No
    - o Do Not Know

28. Has your organization identified areas that may be attractive or vulnerable for cyber attack or breach?
    - o Yes
    - o No
    - o Plan to soon

- Do Not Know

29. Have you conducted conversations with staff, board members, volunteers, and others regarding cyber security?
    - Yes
    - No
    - Plan to soon
    - Do Not Know

30. Have you documented the identities and credentials of the staff members that access to files, databases, and other electronic information?
    - Yes
    - No
    - Plan to soon
    - Do Not Know

31. Do you inform staff about cybersecurity policies, practices, and procedures?
    - Yes
    - No
    - Plan to soon
    - Do Not Know

32. Do you inform third-party vendors and partners about cybersecurity policies, practices, and procedures?
    - Yes
    - No
    - Plan to soon
    - Do Not Know

33. With survivor and other sensitive information stored in digital files, is this information protected by any of the following? (check all that apply)
    - ☐ Secure Passwords
    - ☐ Limited Staff Access
    - ☐ Secure Software
    - ☐ Third-Party
    - ☐ Do Not Know
    - ☐ Other (fill-in)

34. Do you have a policy for the destruction of digital files and information?
    - Yes
    - No
    - Plan to soon
    - Do Not Know

35. Has your organization experienced a cybersecurity breach or attack?

- Yes
- No
- Do Not Know

36. If yes, was the situation clearly understood by all?
    - Yes
    - No
    - Do Not Know

37. Did you feel or do you feel adequately prepared for a cybersecurity breach or attack?
    - Yes
    - No
    - Do Not Know

38. Do you have access to resources and experts to help your organization with cyber security?
    - Yes
    - No
    - Do Not Know

39. Contact Information (optional)
    Name:
    Organization Name:
    State:
    Phone:
    Email:

An online version of this survey is available. Go to [LINK]

The identities of participating organization and their responses to this survey will be anonymous and kept in a secure location. Results reported in the final analysis will not include any identifying information about any organization participation in this study.

Thank you for filling out this survey. The information you provide is the first step in helping organizations working with victims of violence stay safe in a digital world. If you would like to receive the final report from this survey, please indicate is the first step in helping organizations like yours address the complex landscape of cyber security.

Appendix I: Pilot Review Round Two – Email Script

On January 5, 2016, round two of the pilot review began with the following email to each participant.

Dear Pilot Group -

Happy New Year! Thank you again for participating in the "pilot" phase of this research study aimed at identifying the current state of information security within organizations working with victims of violence.

I'm happy to report that **Round One** is now complete. Attached is a full report. Thank you all for providing helpful comments, feedback, and suggestions - the final survey will be significantly improved thanks to you.

We are now moving onto **Round Two.** If you have a moment to continue simply:
1. Open or download the attached results report;
2. Take a moment to review the comments from all the respondents;
3. Send **new or additional** comments/suggestions by **January 15, 2016**.

What's coming next?
At the end of **Round Two**, comments will be incorporated into the survey then submitted to the IRB for final approval. Once approved the goal is to launch the final survey, with the help of the NNEDV, Thorn, and Demand Abolition, on or before February 1, 2016.

Thank you again for your time and support of this study. Your input **continues** be invaluable in helping to find new and efficient ways for organizations working with victims of violence to navigate the complexities of cybersecurity. As a reminder, your participation is entirely voluntary, and you can stop participating at any time with no consequences.

Questions: please contact me at kmisata@purdue.edu or (617) 650-0601.

Appendix J: Pilot Review – Final Results

The following report includes all comments and reccomenations received from the pilot group particpating in this study. Results have been compiled from two rounds of feedback from 13 pilot respondents.

Round One Results

Q1: Consent Statement				
No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
6				
Comments:				

Q2: What type(s) of victims or survivors does your organization serve? (check all that apply) • **Domestic Violence** • **Sexual Assault** • **Human Trafficking** • **Stalking** • **Other (fill-in) _____**				
No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
6				
Comments: • **If you send this out to our lists, then some of them are going to want to answer: all crime victims.** • **May want to consider adding "refugee" since it is common these days (sadly). Political refugees in particular are often hunted by governments.** • **I think you should have separate item regarding cyber security to determine whether IT security is managed by someone explicitly trained and tasked to take on those duties, or if this gets lumped into general IT management duties. Also, as you allude later to surveillance cameras, should physical security monitoring/surveillance management be included in this item (or have a question of its own).**				

Q3: What is the size of your organization? • **Number of Full-Time Employees _____** • **Number of Part-Time Employees _____** • **Number of Volunteers _____**				
No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **Not sure if folks (or I) know the difference between IT consultant or third-party vendor.**
- **(Round Two) Do you want to include consultants?**

Q4: Who manages your technology, computer systems, cyber security?

1. **Full-time information technology employee**
2. **Part-time information technology employee**
3. **Full-time employee with information technology as part of their job**
4. **Part-time employee with information technology as part of their job**
5. **Volunteer**
6. **Information technology consultant**
7. **Third-party vendor**
8. **Other _____**
9. **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3	1	1		

Comments:

- **Use of security, information security and cyber security throughout the survey feels inconsistent. Also, what is the difference between InfoSec and CyberSec? I'm not sure even those of us who do this for a living are in agreement, seems like this would be very confusing for a non-security professional to sort out. Even an innocuous question like #4 could cause confusion: *Who manages your technology, computer systems, cyber security?* If I were answering I'd be wondering - what is the difference between tech, computers and cybersec? What is a respondent thinks since it's multiple, things, there must be multiple people managing them? In a bigger organization this would be true, one team would do ops (computer systems) and another would focus on security (security/risk) and there might even be a third for sec-ops. But in a small org, it may all be lumped into a single group/person - so asking "Who manages the computers and IT" may be an easier one for people to answer.**
- **The answer could be a few of these. Not sure if you want to say "check all that apply" or provide some additional options. Some places have a volunteer IT person, some have a part-time IT person, and others have a part-time or full-time third party company that is essentially IT people/person with their own business. So I could see people unsure of what to answer or wanting to check multiple options.**
- **Add "primarily" before manages.**
- **Our technology is split between 3 soon to be 2 vendors. We trust that they can assess risk and prevent hacks to our system, however I don't know enough about cyber security to ensure they are fully protecting us.**
- **(Round Two) I would encourage a "check all that apply." I think that**

would minimize the confusion between the three different areas one of the respondents was concerned about.

Q5: What is your annual budget?

10. Less than $75,000
11. $75,000 - $149,999
12. $150,000 - $349,999
13. $350,000 - $499,999
14. $500,000 - $999,999
15. Greater than $1,000,000
16. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4				1

Comments:

- **Confirm if this is the annual budget of the IT department or the entire organization.**
- **Maybe add one more level $5,000,000+**

Q6: Where is the mission of your organization posted? (check all that apply)

- **Organization website**
- **Hardcopy materials - marketing, promotional, recruiting, educational, etc.**
- **Social media**
- **Other _____**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4				1

Comments:

- **Not sure why this question is here…not that you shouldn't ask it, but my initial thought was um, why do you want to know? It's not really about tech security.**
- **Unclear why this is asked. If needed for your reference, suggest asking this as part of the survey request, not in the survey itself.**
- **I'd ask whether it is accessible as part of public record (e.g., state or federal filing as non-profit, etc.) separate from organization marketing collateral.**

Q7: What computer operating systems does your organization use? (check all that apply)

- **MAC (Apple)**
- **Microsoft Windows (PC)**
- **Linux (PC)**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4		1		

Comments:

Q8: What technologies does your organization use? (check all that apply)

- **Desktop computers**
- **Laptop, notebook computers**
- **iPads, tablets**
- **Smart-phones (e.g. iPhone, Android, Galaxy, etc.)**
- **Land-line phones**
- **Fax machines**
- **Digital cameras**
- **Surveillance / monitoring Cameras**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4		1		

Comments:

- **Landline phones are pretty specific. Did you want to include VoIP/landline phone or perhaps add VoIP as another option?**
- **Smartphones is specific. Did you want to include just regular cell phones?**
- **Do you want to include VOIP services? A lot of program are using basic cell phones because of the additional privacy risks they have to think about with smartphones so that might be good to add too.**
- **Might say "What device technologies…" to differentiate from security technologies, services, etc. This question should come before 7 since it establishes whether they have computers with operating systems. Would be nice if it was contextual, so if someone did not check desktops/laptops/tablets they would not get the operating system question.**
- **Maybe add printers, external hard-drives to the choices**
- **(Round Two) I have no idea what VoIP means. But if it means basic cell phones (like flip phones?) I would include that as an option. It's very popular among advocates to use.**

Q9: Does your organization currently use any of the following security technologies? (check all that apply)

- **Firewall (e.g. Comodo Internet Security, IPFilter, Netfilter, Norton360, Online Armor, etc.)**
- **Anti-virus software (e.g. Webroot SecureAnywhere Antivirus, McAfee AntiVirus, Kaspersky AntiVirus, etc.)**
- **Password protection software (e.g. Dashlane 3, Sticky Password, Password Boss, LogMeOnce, etc.)**
- **VPN - virtual private network (e.g. Private Internet Access, Hotspot Shield Elite, PureVPN, etc.)**
- **Other proxy services (e.g. Tor, HideMyAss, CyberGhost, BTGuard, etc.)**
- **Cloud storage services (e.g. Google Drive, Dropbox, Apple iCloud, Microsoft OneDrive, etc.)**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
1	4	1		

Comments:

- **I'm not sure folks would consider cloud storage services as a security thing?? More like a software service alternative??**
- **2 things re: the mention of cloud storage services: 1) It doesn't seem to fit as a security technology and I'm not sure I would want programs to see it that way. We don't tell programs not to use cloud services, but we do ask that they carefully think through what data they store within cloud services and to be very cautious about their contracts when storing survivor data. Depending on what data they are including and what contract & features they have on the service, it could be more of a security risk to survivor data. 2) the examples provided of cloud services are one type – but I could see these confusing programs because they also regularly use cloud services that are stand-alone business to store and back-up their data. I think this is different because some programs may use Google Drive or Dropbox to share non-sensitive work files, but the cloud services that is housing their database is holding all of their agency files. If a program just checks this without further detail, I'm not sure you'd be able to assess from the answer the level of potential security.**
- **May not be too technical depending on who is filling this out. But I think it's OK to mention getting technical help from IT support in the question.**
- **It is a little technical and we don't full know what services we use to protect our organization.**
- **I'd include an item for file encryption separate from storage solutions (e.g. PGP, Silent Circle, etc.).**
- **This may require some explanation; respondents may not know what these things are.**

- **Maybe add follow-up asking which specifically.**

Q10: How does your staff access the Internet? (check all that apply)

- **Wired connection (Ethernet)**
- **Internal wireless internet**
- **External mobile hotspot**
- **Public Wi-Fi**
- **Home Wi-Fi**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **I'd add an item for non-Wi-Fi mobile telephone access (cell data link).**

Q11: Does your staff access internal electronic documents from outside the organization?

17. No
18. Yes
19. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3		2		

Comments:

- **I think "outside the organization" should be defined. Maybe to say "outside of the office," or "remotely."**
- **Do you want to know about accessing any types of documents outside of the office or sensitive data specifically?**
- **Maybe add outside physical location.**

Q12: What social media does your organization use? (check all that apply)

- **Twitter**
- **Facebook**
- **LinkedIn**
- **Google+**
- **Snapchat**
- **Tumblr**
- **Instagram**
- **Pinterest**
- **YouTube**
- **Vine**
- **WhatsApp**
- **Flickr**
- **Other _____**
- **None**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **Add "kik" (messenger)**

Q13: Who in your organization is responsible for managing the organization's social media channel(s)?

20. **Dedicated full-time employee**
21. **Dedicated part-time employee**
22. **Shared across several employees**
23. **Contractor**
24. **Volunteer**
25. **Third-party vendor**
26. **Other _____**
27. **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4				

Comments:

- **I was a bit confused why employees was split into full-time, part-time and shared. It could be all of the above. Are you trying to assess if programs have staff whose entire job is to do social media?**
- **(Round Two) Might be helpful to make this a "check all that apply." We have multiple people who are responsible for social media.**

Q14: For what purpose(s) does your organization use social media? (check all that apply)

- **Awareness**
- **Education**
- **Fundraising**
- **Outreach**
- **Employee or volunteer recruiting**
- **Event announcements**
- **No defined purpose**
- **Other _____**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3				2

Comments:

- **Do some orgs use social media as a tool to directly communicate to victims for support/counseling? I bet they do. Might be a good to include.**
- **Add "programs"**

Q15: Does your organization have policies regarding social media use by the following? (check all that apply)

- **Staff**
- **Volunteers**
- **Victims / survivors**
- **External partners (individuals or organizations)**
- **Other stakeholders (e.g. board members, advisors, etc.)**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **I think programs can get really confused by this. Many will have policies in place – but various policies. There could be policies on staff's appropriate use of social media (reminders not to share identifying information or to friend survivors) or policies on staff's personal use of social media during work hours. There can also be policies on survivor's use of social media that restricts their use completely that just asks that they avoid "checking in" and sharing location and photos, or other variations. I think there is a big difference between staff use when they have sensitive information and survivor's use.**
- **Our policies only cover employees because we are a statewide sexual assault coalition.**
- **Specify "HR" policies might make this more clear.**

Q16: Do you feel you need more information regarding technology and cyber security?

28. No
29. Yes
30. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3		2		

Comments:

- **Pretty high-level question opens to all sorts of interpretation. Even though you may be getting at a need for more education with this question, I'd be tempted to phrase it as "more help" since information and education can overwhelm (do I need it? I don't know, or know what to do with it, or have time to take or process the info), but they know they need help.**

Q17: What type(s) of training are most effective in your organization? (check all that apply)

- **On-site in-person training**
- **Off-site in-person training**
- **Web-based training**
- **Hardcopy training materials**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3		1		

Comments:

- **We know that regardless of the org, in-person training is most effective, we know that web-based training has terrible retention, we know that everyone throws printed stuff away. I'd be more interested in whether they had any training and what type, so phrase it like "What form of training does your organization use? (check all that apply)", with an option for "None", and then ask if it was useful/improved security behavior.**
- **(Round Two) I disagree with the other review. I think this question makes sense the way it is.**

Q18: What are barriers to improving your organization's cyber security? (check all that apply)

- **Lack of funding**
- **Lack of time**
- **Lack of knowledge or understanding of technology**
- **Lack of resources**
- **Focus on other priorities**
- **Resistance by staff or other stakeholders**
- **No need**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3		1		1

Comments:

- **So a lack of funding/time and lack of resources might be the same thing – just a thought.**

Q19: Are the computers, laptops, cell phones, and other technologies in your organization inventoried?

31. All
32. Some
33. None
34. Do Not know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3	1	1		

Comments:

- **Add "belonging to".**
- **Define "inventoried".**
- **(Round Two) I still think "inventoried" needs to be identified.**

Q20: If inventoried, is it documented?

35. No
36. Yes
37. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
1		5		

Comments:

- **Not sure what the difference is between inventoried & documented. I would think they're the same??**
- **Not sure what "criticality" means.**

- **This doesn't make sense to me.**
- **Wouldn't inventorying imply documenting? Might not need this question if the one above just includes "inventoried and documented".**
- **Can you differentiate between document and inventory?**
- **The "it" is unclear here. Do you mean is the inventory documented? or do you mean that there's a document describing the inventory? Might be helpful to use a proper noun rather than "it" here.**
- **(Round Two) If you expand on this just a little it would be clearer. For example. "If inventoried, is it documented and stored?"**

Q21: Is the software used by your organization inventoried?

38. No
39. Yes
40. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4	1	2		

Comments:

Q22: Has your organization assigned a criticality to the hardware and software being used within the organization?

41. No
42. Yes
43. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
2	3	2		

Comments:

- **I'm not sure what this means and I think programs may not fully understand.**
- **Might have to explain it a bit, call it assign levels of criticality to the various hardware, software and infrastructure used by the organization. Then possibly an example: e.g. a list such as: support phones are top tier critical to our org, volunteer database is 2nd tier, etc.).**
- **Criticality????**
- **(Round Two) I agree with the other comments.**

Q23: Does your organization have policies for power or Internet outages?

44. No
45. Yes
46. Do Not Know

No Change	Language Too	Confusing	Does Not Fit	Other

	Technical		Objective	
5		1		

Comments:

- **Just a thought about the word policy – when most agencies think of policies, it's written down policies or something official. In some cases, they'll have a general plan of what should be done even if it's not written down. The reason I bring this up is that an agency might have a plan on what to do if they lose power/internet (everyone works from home! Or we light candles!) but may not have an actual policy around this. Depending on what you're trying to ask for, you may want to wordsmith this a bit.**
- **This is such an interesting question. I don't know if we have a policy on this!! I'm curious, if assessing for security, why this question is here over one asking about policies for maintaining access levels or something. But I may be ignorant to something important here re: power outages and security.**

Q24: Does your organization have written policies for security at your organization?

47. No
48. Yes
49. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3		3		1

Comments:

- **I'd clarify what "security" means. It could mean a lot of different things. Someone answering this could say: yes, we have a security plan because we know what to do when an abuser shows up. Or we have security because the local police drive by every now and then? I'd define or describe more what you mean?**
- **This is a huge question. Programs will have a ton of policies that could be defined as security. I would narrow this and make it more specific to what you want to know. A lot of shelters have policies about how you answer the door (one shelter comes to mind that I've visited that has 2 entrances. Both bullet proof. Both mirrored so you can't see in. Only one opens at a time. You show yourself to the camera and announce who you are and they open the first set of doors. Only after they close behind you do the second set of doors open. At one of the shelters I worked at, you had to have a pin to get in and we had strict rules on what to do if someone came knocking who didn't have the pin.) These are all in the name of security. So are policies around communicating with police, contacting a survivor at a home phone number, etc. All about "security" but not specific to their technology or data.**
- **Does your organization have written, accessible policies…"**

- **I'd have two separate questions about this, one for physical security, another for IT security.**
- **Need to specify if security is "technical" or "physical" security.**
- **Base on the survey content it feels like you meant cyber security in Q24.**
- **(Round Two) Defining security would definitely be helpful.**

Q25: Do your polices include cyber security?

50. No
51. Yes
52. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3	1	1		1

Comments:

- **Not in the online survey version.**
- **Reword questions "Do your policies defined cyber security?**
- **Maybe give examples folks might say no before they get to the question if they answered yes, but seeing the options they would have answered yes.**

Q26: If yes, which technologies do these policies include? (check all that apply)

- **Use of computers, laptops, and tablets issued by the organization**
- **Use of cell phones issued by the organization**
- **Use of personal cell phones, laptops and other technologies**
- **Use of social media for organizational purposes**
- **Use of personal social media in reference to working for the organization**
- **Use of public Wi-Fi**
- **Protection of passwords**
- **Accessing files and sensitive electronic documents**
- **Protection of backups, disks, tapes, software, manual**
- **Other** _____
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3	1	1		1

Comments:

- **Not in the online survey version.**
- **Would include "cyber security" before "policies" to remind people of the context.**
- **(Round Two) I think this is fine.**

Q27: Who in your organization is responsible for cyber security for the organization? (check all that apply)

- **Executive Director**
- **Manager / Director**
- **Staff Member**
- **Consultant**
- **Volunteer**
- **Third-Party Vendor**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **This is going to be a bit confusing because of different understanding what cyber security means. I'm not quite sure how to answer this.**
- **Not sure what the difference between a consultant and a Third-Party vendor – maybe clarify or eliminate one.**

Q28: Who in your organization is responsible for the legal requirements for cyber security, such as privacy rights? (check all that apply)

- **Executive Director**
- **Manager / Director**
- **Staff Member**
- **Consultant**
- **Volunteer**
- **Third-Party Vendor**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3				1

Comments:

- **I'm not sure what you mean by privacy rights.**
- **I think this needs to be explained more.**
- **Add "Board of Directors"**
- **Might be happening at multiple levels.**

Q29: Are the legal requirements regarding cyber security understood by those responsible?

53. No
54. Yes
55. Do Not Know

No Change	Language Too	Confusing	Does Not Fit	Other

	Technical		Objective	
4		1		

Comments:
- **Not sure what you mean by legal requirements.**
- **Legal requirements are unclear here.**

Q30: Has your organization identified areas that may be attractive or vulnerable for a cyber attack or breach?
56. No
57. Yes
58. Not yet, but will soon
59. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4	1			

Comments:
- **Perhaps also add "identified areas or practices"??**
- **Would love feedback on this.**
- **This could be scary to some people who are responding.**
- **Maybe add follow-up asking to describe.**

Q31: Has your organization experienced a cybersecurity attack or breach?
60. No
61. Yes
62. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

Q32: If yes, was the situation understood by your organization?
63. No
64. Yes
65. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
2		1		

Comments:
- **I'm not sure that this will be clear. Do you mean that the org understood how it happened in the first place? Or how it was fixed? How it's been addressed so it won't happen again? Or how it impacted survivor data?**
- **"understood" is pretty vague. If you're trying to find out if they believe they now know how to prevent it from happening again, it could be more**

directly asked. Maybe give a few options. If yes, what is your new level of preparedness should this kind of attack reoccur? We learned a great deal from it and are ready to defend against it - We learned somewhat from it and can reduce the chance of lost information or time before we're back in operation -We learned very little but are at least more aware of and alert to the problem -We are as helpless as ever to this attack.

- **Not clear what is being asked here. Probably also more complicated than yes/no response.**
- **Understood?**
- **(Round Two) Not sure what is meant by understood.**

Q33: Does your organization consider itself prepared to handle a cybersecurity breach or attack?

- **No**
- **Yes**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4				2

Comments:

- **May be redundant depending on what changes you make to previous questions based on my comments. Otherwise no change.**
- **May want to score this on a scale of how well prepared.**

Q34: Has your organization conducted cybersecurity workshops or trainings with staff, volunteers, and other stakeholders?

66. No
67. Yes
68. Plan to Soon
69. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

- **I'd change "trainings" to "training."**
- **I'd add a questions – if answer is yes, who conducted this training.**

Q35: Does your organization document who has access to files, databases, and other electronic information?

70. No
71. Yes
72. Do Not Know

No Change	Language Too	Confusing	Does Not Fit	Other

	Technical		Objective	
4		1		1
Comments:				

Q36: Does your organization inform new employees about cybersecurity policies and procedures?

73. No
74. Yes
75. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				
Comments:				

Q37: Does your organization inform third-party vendors, partners, and external stakeholders about cybersecurity policies and procedures?

76. No
77. Yes
78. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4	1	1		
Comments: • **Whose policies, the vendor's or yours?**				

Q38: Regarding the storage of sensitive information, how are these electronic files protected within your organization? (check all that apply)

- **Dedicated hardware (e.g. dedicated computer)**
- **Secure passwords**
- **Limited access**
- **Secure software**
- **Third-party storage (e.g. cloud storage)**
- **Encryption**
- **Biometrics**
- **Other _____**
- **Do Not Know**

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
3	2			1
Comments: • **I'm not sure all these answers help you assess the question. If the question**				

is about ways in which files are protected, then dedicated hardware, third-party storage, secure software, doesn't really make sense to me. They're products, not necessarily protection mechanisms or ways. Does that make sense? I'm also not sure I understand what you mean by dedicated hardware – I think what you're getting at is files are on a dedicated computer or server with no outside access or something…but I think that needs to be defined. I'm also not sure what secure software means either. I also think someone can read this as: yes, my software is secure.

- **Same concern as above with referring to cloud storage as a protection strategy.**
- **May need to explain encryption and biometrics to some people.**

Q39: Does your organization have policies and procedures for the destruction of electronic documents?

79. No
80. Yes
81. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
4	1			1

Comments:

- **I'd add an additional question pertaining to destruction of disks and storage devices taken out of service (including DVDs/CDs/thumbdrives/SDcards).**

Q40: Does your organization have access to external resources and experts to help with cyber security?

82. No
83. Yes
84. Do Not Know

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5		1		

Comments:

Q41: Please provide any additional information regarding the current state of information security within your organization.

No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				

Comments:

Q42: If you would like to receive the results of this survey at the conclusion of this study, please provide your contact information.				
No Change	Language Too Technical	Confusing	Does Not Fit Objective	Other
5				
Comments:				

1. The survey is intended to take participants 10 minutes or less to complete, will the length of the survey and complexity of the questions meet this objective?

    - Yes = 4
    - No = 2
    - Do Not Know = 1

    Other Comments:

    - The survey itself is very quick and a tech/IT guru at the organization might be able to complete it in 10 minutes - but it's too dense for a non-tech. And some questions - like how is the Internet accessed may really trip non-techs up.
    - I definitely think that it will take people longer than 10 minutes to complete.
    - Depends on the person's knowledge and comfort level. I think this is probably a 15-20-minute survey.
    - Although questions were simple, I did not know some of the information and I had to consult with my Executive Director to answer the questions.
    - In general, I think the time will be sufficient. There are going to be some who will probably require more time than 10 minutes.
    - Might add some clarification and/or examples to questions so that respondents aren't spending time trying to figure out what the question is asking.
    - (Round Two) I think it will take at least 15 minutes.

2. Does the order of the questions make sense?

    - Yes = 5
    - No
    - Do Not Know = 1

    Other Comments:

    - I didn't take the online version, so I'm not sure if there's contextual asking, like the comment I made on question 8 above. I think overall it

flowed, but there was one instance (26) where social media cybersec policy was in a list and yet social media policy was asked about prior. It took me a moment to consider that the first instance of the question was around general social media policy, which could include tone and types of conversations, identifying yourself as a member of your org, etc.

3. Please provide suggestions or comments to a specific survey question(s) – ensure to include the question number.
    - Overall the level of many of these questions seems pretty deep/tech for non-tech respondents. Which would result in a lot of "Don't Knows" or attempts to answer that aren't accurate.
    - Use of security, information security and cybersecurity throughout the survey feels inconsistent. Also, what is the difference between InfoSec and CyberSec? I'm not sure even those of us who do this for a living are in agreement, seems like this would be very confusing for a non-security professional to sort out. Even an innocuous question like #4 could cause confusion: *Who manages your technology, computer systems, and cyber security?* If I were answering I'd be wondering - what is the difference between tech, computers and cybersec? What is a respondent thinks since it's multiple, things, there must be multiple people managing them? In a bigger organization this would be true, one team would do ops (computer systems) and another would focus on security (security/risk) and there might even be a third for secops. But in a small org, it may all be lumped into a single group/person - so asking, "Who manages the computers and IT" may be an easier one for people to answer. (NOTE: this response was also added to comments under Q4).
    - Can provide more details on all the questions I didn't mark as "No Change" - but the top level points are all the same. Please do let me know if you'd like expansion on any specific question though.
    - Answers to questions 4 and 13 may be multiple people, the answers are all singular.

4. Please provide any additional comments or suggestions regarding the survey or the process.

    - You ask quite a bit of social media questions – particularly around the purpose of social media, and I'm not sure how it fits w/ an security assessment. In a way, it could be a security issue, but whether an org uses it, how many and why may not necessarily translate to better or worse security. So I guess my feedback is what information are you trying to learn here?
    - Not a lot of people are going to be able to understand these questions. I think you might want include a definitions/terms document? For example, cyber security isn't really defined anywhere, and I think folks are each going to have a different understanding of what that means. This may skew what you get.

One of the things we do when we ask a question that we think will confuse people is we define or explain or describe it within the question so it's clearer.

- Over the years of doing lots of survey to the field I have found 2 things helpful. For each question:
    - I think, if I was not very bright, or I was too bright and for every question I have 3 answers for you that could be correct based on how I read your question, does this question, in any way, confuse me?
    - I pretend that I have the answers to them and decide how I would report/analyze/describe the result based on those pretend answers. If I can, then it usually means I have a good question. If it doesn't then I need to work on the question a bit more.
- Starting at Q12 there are a lot of questions on social media and I think it might be worth thinking through what you want to get out of this. A lot of programs have social media accounts but most of them are using them to share non-sensitive data. I'm not sure that the security risks are clearly identified just by knowing the answers to some of this. You may have a very concrete goal that you want to get out of this and I'm just not seeing it, but I couldn't help but wonder about what the security risks were that would be assessed with these. There are definitely programs who may not follow all the best practices with how to use social media appropriately, but we see way more concerns with how programs are collecting, storing, and retaining victim information without understanding security risks than with how they are using social media.
- I think it could be helpful to define some of the terms and make the goal of this very clear. It could also help to identify who you think would be best to fill this out. If it's not the right person, I think you could end up with A LOT of Do Not Knows, which can make the data a lot less useful.
- For any question regarding technology that is deployed (8 9 at a minimum), I would recommend also asking the % deployment of the technology.
- I would recommend asking both whether the organization has experienced an "attack" (DDoS) or a data breach.
- I think even without my comments, it was a solid survey and will inform your objectives nicely. In your opening introduction to the survey on the agree page, it may be useful to include a statement about the desired outcome of the research, even though it's implied, something like— *Our hope is that we'll be able to assist these support organizations in better protecting themselves from data breaches and in doing so, safeguarding victims of violence from fraud or further abuse.*
- Questions 7-11 and 28 are very technical and that's fine, but the survey or instructions should note the responder should consult the IT Department for those answers.
- Great job.
- You should spend more time on the introduction to help people feel comfortable before they start the survey. Some people may be put off or scared by the questions so helping them feel that it's "OK" to respond with "Don't Know" should be stated upfront. Also helping people understand how this will really help them will inspire them to contribute to the survey – we get surveyed all the

time and often I don't answer them because there isn't enough time. If you make the survey easy with a solid reason for filling out, then people will participate.

Results Round Two

- After reviewing the survey and feedback, I think that my biggest takeaway would be to possibly include some additional language up from about the content of the survey so that the recipient of the survey can determine who the right person is to actually complete the survey.
- I agree with other comments that a terminology sheet would be very helpful, especially for those who are not tech people. ☺
- FYI: Information Security (InfoSec) is the practice of protecting information wherever it exists, in networks, on paper, even in people's minds. Cybersecurity (or sometimes computer security) is a subset of that, which deals with just computing security and digital information. The two are often incorrectly used synonymously, but the distinction is important because cyber folks often forget about the places where information exists other than computers. An example: discarded paper patient records taken from a dumpster and used for Medicare fraud. Make sure you're clear on what's being asked about.
- The comment about cloud security raises another potential question: "Do you evaluate your vendors and contractors for their [info/cyber] security?" Many organizations blindly trust vendors, and it's turning out most of the breaches today are coming through unsecure or even malicious vendors.
- What a great bunch of response! Lots of good feedback. Excited to see the next revision.
- I laughed at the comment "Not sure why this question is here… it's not really about tech security." For "Where is the mission of your organization posted?" Please respond with "Because if I change your mission statement to 'badger herder' you'd be upset." No comments to add or change. Well done.

Appendix K: General Survey – Email Scripts

To: NNEDV, Thorn, Demand Abolition

From: Kelley Misata kmisaa@purdue.edu

Subject: Purdue University Research Study on Information Security In Crisis Organizations

You are invited to participate in a research study aimed at identifying the current state of information security within organizations working with victims of violence. The goal is distributing the following summary including survey link to crisis organizations in your database.

If you choose to participate your role in facilitating this survey will be invaluable. However, please know that your participation is completely voluntary, and you can stop participating at any time with no consequences.

To participate

1. Initial Email to Crisis Organizations: send the following summary and survey link to all crisis organizations in your database;
2. Reminder Email #1: in approximately 10 business days, send reminder email #1 – we will send you a reminder regarding this at least 2 business days prior;
3. Reminder Email #2: approximately 20 business days after step 1, send reminder email #2 – we will send you a reminder regarding this at least 2 business days prior.

Please note participation in the survey is also voluntary therefore crisis organizations participation will have the opportunity to opt out at any time with no penalty or consequence.

If you have questions please contact Kelley Misata at kmisata@purdue.edu, (617) 650-0601, or Eugene Spafford at spaf@purdue.edu.

1. Email Invitation to Crisis Organizations

From: Kelley Misata
Reply-to Email: kmisata@purdue.edu
Subject: Purdue University Research on Information Security In Crisis Organizations

You are invited to participate in a survey that is being conducted by researchers at Purdue University, to analyze the current state of information security within organizations working with victims of domestic violence, stalking, and human trafficking in the United States. Your participation in this survey is completely voluntary, and you can stop

participating at any time with no consequences. This survey will assist in understanding the current state of information security within crisis organizations working victims of violence, and your assistance is greatly appreciated. You must be 18 years of age to participate, and all results will be maintained in an encrypted system at Purdue University.

If you have questions please contact Kelley Misata at kmisata@purdue.edu, 617-650-0601, or Eugene Spafford at spaf@purdue.edu. The survey should take less than 10 minutes for you to complete.

Follow this link to the Survey: [LINK]
Or copy and paste the URL below into your internet browser: [URL}

Thank you for your time and for participating in this important survey.
Kelley Misata

2. Reminder Email #1 to Crisis Organizations

From: Kelley Misata
Reply-to Email: kmisata@purdue.edu
Subject: Survey Reminder: Purdue University Research on Information Security In Crisis Organizations

Following up on our email a few days ago, regarding an invitation to participate in a survey that is being conducted by researchers at Purdue University, to analyze the current state of information security within organizations working with victims of domestic violence, stalking, and human trafficking in the United States.

If you have completed the survey, thank you! Your input in this study is invaluable.

If you have not yet completed the survey, we need your help. Simply, follow this link to the Survey: [LINK]
or copy and paste the URL below into your internet browser: [URL}

As a reminder, your participation in this survey is completely voluntary, and you can stop participating at any time with no consequences. This survey will assist in understanding the current state of information security within crisis organizations working victims of violence, and your assistance is greatly appreciated. You must be 18 years of age to participate, and all results will be maintained in an encrypted system at Purdue University.

If you have questions please contact Kelley Misata at kmisata@purdue.edu, 617-650-0601, or Eugene Spafford at spaf@purdue.edu. The survey should take less than 10 minutes for you to complete.

Thank you for your time and for participating in this important survey.
Kelley Misata

3. Reminder Email #2 to Crisis Organizations

From: Kelley Misata
Reply-to Email: kmisata@purdue.edu
Subject: Final Reminder: Purdue University Research on Information Security In Crisis Organizations

Following up on our email a few days ago, regarding an invitation to participate in a survey that is being conducted by researchers at Purdue University, to analyze the current state of information security within organizations working with victims of domestic violence, stalking, and human trafficking in the United States.

If you have completed the survey, thank you! Your input in this study is invaluable.

If you have not yet completed the survey, we need your help. Simply, follow this link to the Survey: [LINK]
or copy and paste the URL below into your internet browser: [URL} Please note, the survey will close in 5 business days.

As a reminder, your participation in this survey is completely voluntary, and you can stop participating at any time with no consequences. This survey will assist in understanding the current state of information security within crisis organizations working victims of violence, and your assistance is greatly appreciated. You must be 18 years of age to participate, and all results will be maintained in an encrypted system at Purdue University.

If you have questions please contact Kelley Misata at kmisata@purdue.edu, 617-650-0601, or Eugene Spafford at spaf@purdue.edu. The survey should take less than 10 minutes for you to complete.

Thank you for your time and for participating in this important survey.
Kelley Misata

Appendix L: Final Survey

The following is the general survey based on the feedback provided by the pilot group and approved by the IRB.

Q1: Thank you for participating in a research study conducted by Purdue University. The objective of this study is to identify the current state of information security (risks, opportunities, and priorities) within organizations working with victims of violence. These identifications will be achieved by analyzing the current state of information security of crisis organizations against a recognized cyber security framework.
Our intention is that we will be able to assist these organizations in better protecting themselves from information security breaches and in doing so, safeguard victims of violence.
To help you, we wanted to give you a few important messages about the survey:

- The survey should take less than 15 minutes to complete.
- Answering "Do Not Know" is a good thing if you find yourself unable to answer a question.
- The terms "Information Security" and "Cyber Security" are used throughout – to help keep things clear, "information security" is used and defined as the practice of protecting information wherever it exists including cyber space.
- Some of the questions in the survey use some technical language, we have tried to provide definitions and examples where possible to help you – however, if you do not know an answer remember selecting "Do Not Know" is appropriate.
- No information identifying your organization will be captured, therefore, please feel comfortable with answering "Do Not Know" or skipping a question.
- If you choose not to participate, you can withdraw at any time during the survey without penalty or consequence. If you wish to withdraw, you may stop answer the online survey by closing out of the Qualtrics survey window or by choosing "Do Not Agree" below.

If your organization has international operations, please fill out the survey based on operations within the United States only.

Thank you again for your participation and time. If you have questions, comments or concerns about this study, please contact:
Dr. Eugene Spafford: (765) 494-7825 or spaf@purdue.edu
Kelley Misata: (617) 650-0601 or kmisata@purdue.edu

85. I Agree
86. Do Not Agree

Q2: What type(s) of victims or survivors does your organization serve? (check all that apply)

- Domestic Violence
- Sexual Assault
- Human Trafficking
- Stalking
- Refugees
- Other (fill-in) _____

Q3: What is the size of your organization?

- Number of Full-Time Employees _____
- Number of Part-Time Employees _____
- Number of Volunteers _____

Q4: Who primarily manages the computers and information technology (e.g. Internet connection) in your organization? (check all that apply)

- ❑ Full-time information technology employee
- ❑ Part-time information technology employee
- ❑ Full-time employee with information technology as part of their job
- ❑ Part-time employee with information technology as part of their job
- ❑ Volunteer
- ❑ Information technology consultant
- ❑ Third-party vendor
- ❑ Other _____
- ❑ Do Not Know

Q5: What is the total annual budget of your organization?

87. Less than $75,000
88. $75,000 - $149,999
89. $150,000 - $349,999
90. $350,000 - $499,999
91. $500,000 - $999,999
92. $1,000,000 - $4,999,999
93. Greater than $5,000,000
94. Do Not Know

Q6: Where is the mission of your organization posted? (check all that apply)

- Organization website
- Hardcopy materials - marketing, promotional, recruiting, educational, etc.
- Social media
- Other _____

Q7: What technologies does your organization use? (check all that apply)

- Desktop computers
- Laptop, notebook computers
- External hardrives
- iPads, tablets
- Smart-phones (e.g. iPhone, Android, Galaxy, etc.)
- Cellphones (e.g. flip-phones)
- Land-line phones
- VoIP (e.g Voice over Internet)
- Fax machines
- Printers
- Digital cameras
- Surveillance / monitoring Cameras
- Other _____
- Do Not Know

Q8 What computer operating systems does your organization use? (check all that apply)

- MAC (Apple)
- Microsoft Windows (PC)
- Linux (PC)
- Other _____
- Do Not Know

Q9: Does your organization currently use any of the following security technologies? (check all that apply)

- Firewall (e.g. Comodo Internet Security, IPFilter, Netfilter, Norton360, Online Armor, etc.)
- Anti-virus software (e.g. Webroot SecureAnywhere Antivirus, McAfee AntiVirus, Kaspersky AntiVirus, etc.)
- Password protection software (e.g. Dashlane 3, Sticky Password, Password Boss, LogMeOnce, etc.)
- VPN - virtual private network (e.g. Private Internet Access, Hotspot Shield Elite, PureVPN, etc.)
- File encryption (e.g. GPG, PGP, Trucrypt, etc.)
- Other proxy services (e.g. Tor, HideMyAss, CyberGhost, BTGuard, etc.)
- Other _____
- Do Not Know

Q10: How does your staff access the Internet? (check all that apply)

- Wired connection (Ethernet)
- Internal wireless internet
- External mobile hotspot
- Cellular data connection
- Public WiFi
- Home WiFi
- Other _____
- Do Not Know

Q11: Does your staff access organizational electronic documents from outside the premises?

95. No
96. Yes
97. Do Not Know

Q12: What social media does your organization use? (check all that apply)

- Twitter
- Facebook
- LinkedIn
- Google+
- Snapchat
- Tumblr
- Instagram
- Pinterest
- YouTube
- Vine
- WhatsApp
- Flickr
- Kik messenger
- Other _____
- None
- Do Not Know

Q13: Who in your organization is responsible for managing the organization's social media channel(s)? (check all that apply)

- ❑ Dedicated full-time employee
- ❑ Dedicated part-time employee
- ❑ Shared across several employees
- ❑ Contractor
- ❑ Volunteer
- ❑ Third-party vendor
- ❑ Other _____
- ❑ Do Not Know

Q14: For what purpose(s) does your organization use social media? (check all that apply)

- Awareness
- Education
- Fundraising
- Outreach
- Employee or volunteer recruiting
- Communicating directly with victims
- Programs
- Event announcements
- No defined purpose
- Other _____

Q15: Does your organization have human resources policies regarding social media use by the following? (check all that apply)

- Staff
- Volunteers
- Victims / survivors
- External partners (individuals or organizations)
- Other stakeholders (e.g. board members, advisors, etc.)
- Other _____
- Do Not Know

Q16: Do you feel you need more help understanding technology and information security?

98. No
99. Yes
100. Do Not Know

Q17: In general, what type(s) of training are most effective in your organization? (check all that apply)

- On-site in-person training
- Off-site in-person training
- Web-based training
- Hardcopy training materials
- Other _____
- Do Not Know

Q18: What do you perceive are barriers to improving your organization's information

security? (check all that apply)

- Lack of funding
- Lack of time
- Lack of knowledge or understanding of technology
- Lack of resources (e.g. staff, equipment)
- Focus on other priorities
- Resistance by staff or other stakeholders
- No need
- Other _____
- Do Not Know

Q19: Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies in belonging to the organization?

101. All
102. Some
103. None
104. Do Not know

Q20: Do you know if these items are insured against theft or loss?

105. Yes, they are.
106. No, they are not.
107. Some are.
108. Do Not know

Q21: Is the software used by your organization inventoried?

109. No
110. Yes
111. Do Not Know

Q22: Has your organization identified what hardware and software are critical to your operations?

112. No
113. Yes
114. Do Not Know

Q23: Does your organization have policies or documented plans for power or Internet outages?

115. No
116. Yes
117. Do Not Know

Q24: Does your organization have policies for physical security?

118. No
119. Yes
120. Do Not Know

Q25: Does your organization have policies for information security?

121. No
122. Yes
123. Do Not Know

Q26: If yes, which technologies do these policies include? (check all that apply)

- Use of computers, laptops, and tablets issued by the organization
- Use of cell phones issued by the organization
- Use of personal cell phones, laptops and other technologies
- Use of social media for organizational purposes
- Use of personal social media in reference to working for the organization
- Use of public WiFi
- Protection of passwords
- Accessing files and sensitive electronic documents
- Protection of backups, disks, tapes, software, manual
- Other _____
- Do Not Know

Q27: Who is responsible for information security within the organization? (check all that apply)

- Executive Director
- Manager / Director
- Staff Member
- Consultant
- Volunteer
- Third-Party Vendor
- Other _____
- Do Not Know

Q28: Who in your organization is responsible for the legal requirements for information

security? (e.g. GLBA, HIPPA compliance, protective orders, etc.) (check all that apply)

- Executive Director
- Manager / Director
- Board of Directors
- Staff Member
- Consultant
- Volunteer
- Third-Party Vendor
- Other _____
- Do Not Know

Q29: Are the legal requirements listed in Question 28 regarding information security understood by those responsible?

124. No
125. Yes
126. Do Not Know

Q30: Has your organization identified areas or practices that may be attractive targets or vulnerable for a cyber attack or breach?

127. No
128. Yes
129. Not yet, but will soon
130. Do Not Know

Q31: Has your organization experienced a cybersecurity attack or breach?

131. No
132. Yes, within the past 2 years.
133. Yes, within the past 10 years.
134. Do Not Know

Q32: Does your organization consider itself prepared to handle a cybersecurity breach or attack?

135. No
136. Yes
137. Do Not Know

Q33: Has your organization conducted information security workshops or training with staff, volunteers, and other stakeholders?

138. No
139. Yes
140. Plan to Soon
141. Do Not Know

Q34: If yes or plan to soon, who will conduct the training? (check all that apply)

- Executive Director
- Manager / Director
- Staff Member
- Consultant
- Volunteer
- Third-Party Vendor
- Other _____
- Do Not Know

Q35: Does your organization document who has access to sensitive files, databases, and other electronic information?

142. No
143. Yes
144. Do Not Know

Q36: Does your organization inform or train new employees about information security policies and procedures?

145. No
146. Yes
147. Do Not Know

Q37: Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures?

148. No
149. Yes
150. Do Not Know

Q38: If your organization does use third-party vendors do they inform you of their information security policies and procedures?

151. No
152. Yes
153. Do Not Know

Q39: How is access to electronic files containing sensitive information stored within your organization protected? (check all that apply)

- Dedicated hardware (e.g. dedicated computer)
- Secure passwords
- Encryption software (e.g. Trucrypt)
- Smartcard
- Third-party storage (e.g. cloud storage)
- Biometrics (e.g. finger print reader)
- Other _____
- Do Not Know

Q40: Does your organization have policies and procedures for the destruction of electronic documents?

154. No
155. Yes
156. Do Not Know

Q41: Does your organization have policies and procedures for the destruction storage devices? (e.g. DVDs, CDs, thumbdrives, etc.)

157. No
158. Yes
159. Do Not Know

Q42: Does your organization have access to external resources and experts to help with cyber security?

160. No
161. Yes
162. Do Not Know

Q43: Please provide any additional information regarding the current state of information security within your organization.

Q44: If you would like to receive a statistical summary of this survey at the conclusion of this study, please provide your contact information.

Appendix M: Survey Question Analysis Map to NIST CSF

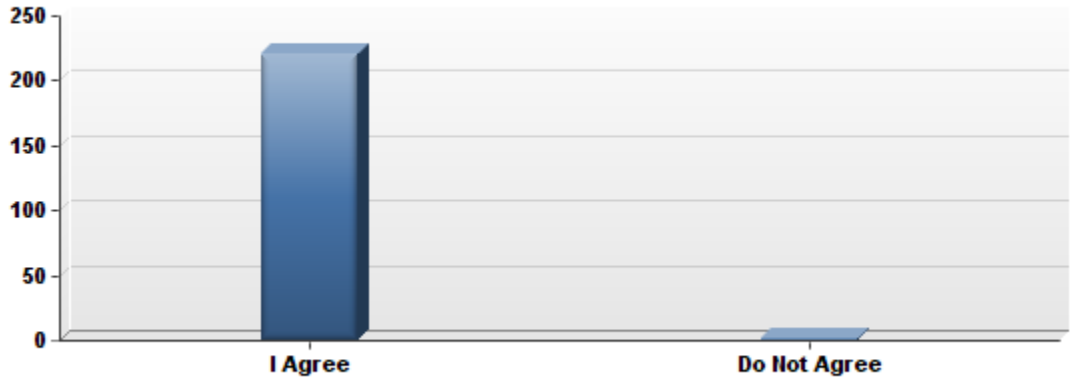
Question		Response Type	NIST
Q2	What type(s) of victims or survivors does your organization serve?	Check All	n/a
Q3	What is the size of your organization?	Fill-In	n/a
			n/a
			n/a
Q4	Who primarily manages the computer and information technology (e.g. Internet connection) in your organization?	Check All	n/a
			n/a
			n/a
			RS.RP-1
Q5	What is the total annual budget of your organization?	Select One	n/a
			n/a
Q6	Where is the mission of your organization posted?	Check All	ID.BE-3
Q7	What technologies does your organization use?	Check All	n/a
			n/a
			n/a
Q8	What computer operating systems does your organization use?	Check All	n/a
Q9	Does your organization currently use any of the following security technologies?	Check All	n/a
			n/a
			n/a
			n/a
Q10	How does your staff access the Internet?	Check All	n/a
			ID.GV-1
Q11	Does your staff access internal electronic documents from outside the premises?	Yes/No	ID.GV-1
			ID.AM-3
			ID.GV-1
Q12	What social media does your organization use?	Check All	n/a
			n/a
			n/a
Q13	Who in your organization is responsible for managing the organization's social media channel(s)?	Check All	n/a
Q14	For what purpose(s) does your organization use social media?	Check All	n/a
Q15	Does your organization have human resources policies regarding social media use by the following?	Check All	n/a
Q16	Do you feel you need more help understanding technology and information security?	Yes/No	n/a
Q17	In general, what type(s) of training are most effective in your organization?	Check All	n/a
Q18	What do you perceive are barriers to improving your organization's information security?	Check All	n/a
Q19	Do you know if your organization has a complete list (inventory) of all computers, laptops, cell phones, and other technologies belonging to the organization?	All/Some/None	ID.AM-1
			ID.AM-2
			ID.AM-5

Q20	Do you know if these items are insured against theft or loss?	Yes/No/Some	ID.AM-1
Q21	Is the software used by your organization inventoried?	Yes/No	ID.AM-2
Q22	Has your organization identified what hardware and software are critical to your operations?	Yes/No	ID.AM-5
Q23	Does your organization have policies or documented policies for power or Internet outages?	Yes/No	ID.BE-4
			n/a
Q24	Does your organization have policies for physical security?	Yes/No	ID.BE-4
			ID.BE-4
			ID.GV-1
			ID.BE-4
			ID.GV-1
Q25	Does your organization have policies for information security?	Yes/No	ID.AM-3
			ID.GV-1
			n/a
			ID.BE-4
			ID.GV-1
			ID.BE-4
			ID.GV-1
			PR.AC-1
Q26	If yes, which technologies do these policies include?	Check All	ID.BE-4
			ID.GV-1
			ID.BE-4
			ID.GV-1
Q27	Who is responsible for information security for the organization?	Check All	ID.AM-6
			ID-GV-2
Q28	Who in your organization is responsible for the legal requirements for information security?	Check All	PR.AT-2
Q29	Are the legal requirements listed in Question 28 regarding information security understood by those responsible?	Yes/No	PR.AT-2
Q30	Has your organization identified areas or practices that may be attractive targets or vulnerable for attack or breach?	Yes/No/Not Yet	ID.RM-1
			ID.RM-1
			ID.RM-1
			ID.RM-1
Q31	Has your organization experienced a cybersecurity attack or breach?	Yes/No	RS.RP-1
			n/a
			ID.RM-1
			ID.RM-1
			ID.RM-1
			ID.RM-1
Q32	Does your organization consider itself prepared to handle a cybersecurity breach or attack?	Yes/No	ID.RM-1
			ID.RM-1
			ID.RM-1
			ID.RM-1
Q33	Has your organization conducted information security workshops or training with staff, volunteers, and other stakeholders?	Yes/No	ID.RM-1
			ID.RM-1
			ID.RM-1

			ID.RM-1
			PR.AT-1
			PR.AT-1
			PR.AT-1
Q34	If yes or plan to soon, who will conduct the training?	Check All	ID.RM-1
			ID.RM-1
			ID.RM-1
			ID.RM-1
Q35	Does your organization document who has access to sensitive files, databases, and other electronic information?	Yes/No	PR.AC-1
			PR.AC-1
Q36	Does your organization inform or train new employees about information security policies and procedures?	Yes/No	PR.AT-1
			PR.AT-1
			PR.AT-1
Q37	Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures?	Yes/No	ID.AM-6
			PR.AT-1
			PR.AT-1
			PR.AT-1
Q38	If your organization does use third-party vendors do they inform you of their information security policies and procedures?	Yes/No	PR.AT-1
			PR.AT-1
			PR.AT-1
Q39	How is access to electronic files containing sensitive information stored within your organization protected?	Check All	PR.AC-1
Q40	Does your organization have policies and procedures for the destruction of electronic documents?	Yes/No	PR.IP-6
Q41	Does your organization have policies and procedures for the destruction of storage devices? (e.g. DVDs, CDs, thumbdrives, etc.)	Yes/No	PR.IP-6
Q42	Does your organization have access to external resources and experts to help with information security?	Yes/No	n/a

Appendix N: Survey Results

Q1: Consent



#	Answer		Response	%
1	I Agree		221	100%
2	Do Not Agree		1	0%
	Total		222	100%

Statistic	Value
Min Value	1
Max Value	2
Mean	1.00
Variance	0.00
Standard Deviation	0.07
Total Responses	222

Q2: What type(s) of victims or survivors does your organization serve? (check all that apply)

#	Answer		Response	%
1	Domestic Violence		**151**	96%
2	Sexual Assault		**116**	73%
3	Human Trafficking		**86**	54%
4	Stalking		**111**	70%
5	Refugee		23	15%
6	Other		20	13%

Other
Adult Protective Services
child sexual abuse
child abuse
elder and disabled
Elder Abuse
sex industry
Robbery, child abuse, stalking, threats, harassment, etc.
Childhood sexual abuse, Elder Abuse
homeless, hungry
immigrant
victims of any violent crime
Survivors of Homicide Victims, Kidnapping, Aggravated Assault
U-Visa's
Child Abuse
crime victims, all types
Comprehensive victim services (includes child abuse and other serious crimes)
substance abuse/addiction
homeless
All violent and non violent state charges in Denver

Statistic	Value
Min Value	1
Max Value	6
Total Responses	158

Q3. What is the size of your organization?

#	Answer		Response	%
1	Number of Full-Time Employees		152	97%
2	Number of Part-Time Employees		129	83%
3	Number of Volunteers		137	88%

Statistic	Value
Min Value	1
Max Value	3
Total Responses	156

Q4: Who primarily manages the computer and information technology (e.g. Internet

connection) in your organization? (check all that apply)

#	Answer		Response	%
1	Full-time information technology employee		30	19%
2	Part-time information technology employee		14	9%
3	Full-time employee with information technology as part of their job		53	34%
4	Part-time employee with information technology as part of their job		9	6%
5	Volunteer		6	4%
6	Information technology consultant		42	27%
7	Third-party vendor		33	21%
8	Other		25	16%
9	Do Not Know		0	0%

Other
I do
Director
We’re part of a larger org that contracts with an IT company to provide support
IT company volunteers
Agency just started with outside firm
Nobody manages it.
full time department
Full time employee with little knowledge not part of job
IT people supplied through the department we are under
Executive Director
Our program is part of a City Police Dept. Where the city employees IT managers, etc.
Executive Director
Staff who happen to be knowledgeable (kinda) in IT
County
We all handle our own databases
Intern
Executive Director
Full time employee with no information technology as part of their job
Program Director with resources to answers as needed
our foundation
Executive Director

Statistic	Value
Min Value	1
Max Value	8
Total Responses	158

Q5: What is the total annual budget of your organization?

#	Answer		Response	%
1	Less than $75,000		6	4%
2	$75,000 - $149,999		11	7%
3	$150,000 - $349,999		15	9%
4	$350,000 - $499,999		11	7%
5	$500,000 - $999,999		25	16%
6	$1,000,000 - $4,999,999		55	35%
7	Greater than $5,000,000		9	6%
8	Do Not Know		26	16%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	8
Mean	5.34
Variance	3.65
Standard Deviation	1.91
Total Responses	158

Q6: Where is the mission of your organization posted? (check all that apply)

#	Answer		Response	%
1	Organization website		144	91%
2	Hardcopy materials - marketing, promotional, recruiting, educational, etc.		144	91%
3	Social media		113	72%
4	Other		19	12%

Other
advocacy and training
Office lobby, in shelter, in client office space
On site
email signature, business cards, etc.
handbooks, everywhere
Throughout Office
At every location
Employee Manuals
Fryers
on the wall in office
all publications
presentations
Every room in our office bldg.

Statistic	Value
Min Value	1
Max Value	4
Total Responses	158

Q7: What technologies does your organization use? (check all that apply)

#	Answer		Response	%
1	Desktop computers		153	97%
2	Laptop, notebook computers		144	91%
3	External hard drives		74	47%
4	iPads, tablets		60	38%
5	Smart-phones (e.g. iPhone, Android, Galaxy, etc.)		102	65%
6	Cellphones (e.g. flip-phones		83	53%
7	Land-line phones		140	89%
8	VoIP (Voice over the Internet)		41	26%
9	Fax machines		146	92%
10	Printers		151	96%
11	Digital cameras		90	57%
12	Surveillance / monitoring cameras		98	62%
13	Other		10	6%
14	Do Not Know		1	1%

Other
Bluetooth devices
scanner
Have internet and intranet
Scanners
Audio/Video recording and storage equipment
copier/scanners
other law enforcement investigative tools, case management tools, vision evidence technology

Statistic	Value
Min Value	1
Max Value	14
Total Responses	158

Q8: What computer operating systems does your organization use? (check all that apply)

#	Answer		Response	%
1	MAC (Apple)		18	11%
2	Microsoft Windows (PC)		155	98%
3	Linux (PC)		3	2%
4	Other		5	3%
5	Do Not Know		1	1%

Other
apple for some

Statistic	Value
Min Value	1
Max Value	5
Total Responses	158

Q9. Does your organization currently use any of the following security technologies? (check all that apply)

#	Answer		Response	%
1	Firewall (e.g. Comodo Internet Security, IPFilter, Netfilter, Norton360, Online Armor, etc.)		114	72%
2	Anti-virus software (e.g. Webroot SecureAnywhere Antivirus, McAfee AntiVirus, Kaspersky AntiVirus, etc.)		132	84%
3	Password protection software (e.g. Dashlane 3, Sticky Password, Password Boss, LogMeOnce, etc.)		51	32%
4	VPN - virtual private network (e.g. Private Internet Access, Hotspot Shield Elite, PureVPN, etc.)		56	35%
5	File encryption (e.g. GPG, PGP, Trucrypt, etc.)		26	16%
6	Other proxy services (e.g. Tor, HideMyAss, CyberGhost, BTGuard, etc.)		5	3%
7	Cloud storage services (e.g. Google Drive, Dropbox, Apple iCloud, Microsoft OneDrive, etc.)		62	39%
8	Other		5	3%
9	Do Not Know		21	13%

Other
Microsoft Intune
RoxioCreatorHome, CyberLincPower
Backblaze
Disaster recovery implementation

Statistic	Value
Min Value	1
Max Value	9
Total Responses	158

Q10: How does your staff access the Internet? (check all that apply)

#	Answer		Response	%
1	Wired connection (Ethernet)		123	78%
2	Internal wireless internet		119	75%
3	External mobile hotspot		20	13%
4	Cellular data connection		44	28%
5	Public WiFi		19	12%
6	Home WiFi		45	28%
7	Other		2	1%
8	Do Not Know		7	4%

Other
Home WiFi for social media only. All client data is accessible on Box only via 2-step verification with Director approval

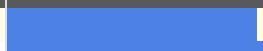
Statistic	Value
Min Value	1
Max Value	8
Total Responses	158

Q11: Does your staff access internal electronic documents from outside the premises?

#	Answer		Response	%
1	No		62	39%
2	Yes		82	52%
3	Do Not Know		14	9%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.70
Variance	0.39
Standard Deviation	0.63
Total Responses	158

Q12: What social media does your organization use? (check all that apply)

#	Answer		Response	%
1	Twitter		83	53%
2	Facebook		142	90%
3	LinkedIn		38	24%
4	Google+		18	11%
5	Snapchat		3	2%
6	Tumblr		6	4%
7	Instagram		29	18%
8	Pinterest		13	8%
9	YouTube		39	25%
10	Vine		4	3%
11	WhatsApp		1	1%
12	Flickr		3	2%
13	Kik messenger		2	1%
14	Other		1	1%
15	None		10	6%
16	Do Not Know		6	4%

Other
blog

Statistic	Value
Min Value	1
Max Value	16
Total Responses	158

Q13: Who in your organization is responsible for managing the organization's social media

channel(s)? (check all that apply)

#	Answer		Response	%
1	Dedicated full-time employee		63	40%
2	Dedicated part-time employee		18	11%
3	Shared across several employees		60	38%
4	Contractor		4	3%
5	Volunteer		8	5%
6	Third-party vendor		3	2%
7	Other		21	13%
8	Do Not Know		10	6%

Other
do not use
PT social media liaison and Director work in tandem
We're part of a larger org with a communications director and dedicated staff
None
the Executive Director
employee, part of her job
n/a
Executive Director
Executive Director
Full time employee with this as part of their job duties
Staff member, but not really a dedicated part of their job
County IT Office
Part time employee with various roles at the agency
No one.
don't have social media
Executive Director
Program Director
Shared across three people (is that several?)
our foundation
Dedicated full-time employee with this as part of the job

Statistic	Value
Min Value	1
Max Value	8
Total Responses	158

Q14: For what purpose(s) does your organization use social media? (check all that apply)

#	Answer	Response	%
1	Awareness	145	92%
2	Education	130	82%
3	Fundraising	112	71%
4	Outreach	120	76%
5	Employee or volunteer recruiting	90	57%
6	Communicating directly with victims	41	26%
7	Programs	57	36%
8	Event announcements	134	85%
9	No defined purpose	6	4%
10	Other	11	7%

Other
building partnerships
Victims reach out to us on social media
n/a
We don't use it.
don't use social media
We discourage use of social media by clients/victims to communicate although we sometimes will get a services request from a client
research
none
We don't use it.

Statistic	Value
Min Value	1
Max Value	10
Total Responses	158

Q15: Does your organization have human resources policies regarding social media use by the following? (check all that apply)

#	Answer	Response	%
1	Staff	111	70%
2	Volunteers	78	49%
3	Victims / survivors	22	14%
4	External partners (individuals or organizations)	10	6%
5	Other stakeholders (e.g. board members, advisors, etc.)	25	16%
6	Other	14	9%
7	Do Not Know	38	24%

Other
No
In Process
not at this time
working on it
confusing...no outside entity has access to our social media accounts. Our Human Resource policies can't dictate to outside entities
No.
no policies
No
shelter residents are asked not to use their smart phones until they have been checked out
No
member programs
None

Statistic	Value
Min Value	1
Max Value	7
Total Responses	158

Q16: Do you feel you need more help understanding technology and information security?

#	Answer		Response	%
1	No		36	23%
2	Yes		95	60%
3	Do Not Know		27	17%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.94
Variance	0.40
Standard Deviation	0.63
Total Responses	158

Q17: In general, what type(s) of training are most effective in your organization? (check all that apply)

#	Answer		Response	%
1	On-site in-person training		128	81%
2	Off-site in-person training		70	44%
3	Web-based training		103	65%
4	Hardcopy training materials		59	37%
5	Other		3	2%
6	Do Not Know		0	0%

Other
Must be in-state training if in person
local conferences

Statistic	Value
Min Value	1
Max Value	5
Total Responses	158

Q18: What do you perceive are barriers to improving your organization's information security? (check all that apply)

#	Answer		Response	%
1	Lack of funding		110	70%
2	Lack of time		76	48%
3	Lack of knowledge or understanding of technology		81	51%
4	Lack of resources (e.g. staff, equipment)		92	58%
5	Focus on other priorities		63	40%
6	Resistance by staff or other stakeholders		21	13%
7	No need		7	4%
8	Other		11	7%
9	Do Not Know		9	6%

Other
Lack of quality NM trainers
Part of a larger org that has different standards for other non-victims services programs and lag behind in understanding our unique needs
I am a branch within a Tribal Nations full computer system, so they don't understand the need for extreme privacy
If there is a need I am not aware...that is why we hire IT professional consultants
Slow Broadband connection
Budget cuts, expensive internet
Understanding by IT professionals about our confidentiality requirements
The City's IT department.
Out dated operating systems
Addressing confidentiality issues with data storage; finding a software database program to gather required data for funders that doesn't cost $30,000 a year in user fees and maintains support

Statistic	Value
Min Value	1
Max Value	9
Total Responses	158

Q19: Do you know if your organization has a complete list (inventory) of all computers,

laptops, cell phones, and other technologies belonging to the organization?

#	Answer		Response	%
1	All		107	68%
2	Some		26	16%
3	None		1	1%
4	Do Not know		24	15%
	Total		158	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	1.63
Variance	1.16
Standard Deviation	1.08
Total Responses	158

Q20: Do you know if these items are insured against theft or loss?

#	Answer		Response	%
1	Yes, they are.		66	51%
2	No, they are not.		6	5%
3	Some are.		14	11%
4	Do Not Know		44	34%
	Total		130	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.28
Variance	1.91
Standard Deviation	1.38
Total Responses	130

Q21: Is the software used by your organization inventoried?

#	Answer		Response	%
1	No		25	16%
2	Yes		77	50%
3	Do Not Know		52	34%
	Total		154	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.18
Variance	0.47
Standard Deviation	0.69
Total Responses	154

Q22: Has your organization identified what hardware and software are critical to your operations?

#	Answer		Response	%
1	No		22	14%
2	Yes		76	49%
3	Do Not Know		56	36%
	Total		154	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.22
Variance	0.46
Standard Deviation	0.68
Total Responses	154

Q23: Does your organization have policies or documented policies for power or Internet outages?

#	Answer		Response	%
1	No		66	43%
2	Yes		51	33%
3	Do Not Know		37	24%
	Total		154	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.81
Variance	0.64
Standard Deviation	0.80
Total Responses	154

Q24: Does your organization have policies for physical security?

#	Answer		Response	%
1	No		17	11%
2	Yes		123	80%
3	Do Not Know		13	8%
	Total		153	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.97
Variance	0.20
Standard Deviation	0.44
Total Responses	153

Q25: Does your organization have policies for information security?

#	Answer		Response	%
1	No		23	15%
2	Yes		103	67%
3	Do Not Know		28	18%
	Total		154	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.03
Variance	0.33
Standard Deviation	0.58
Total Responses	154

Q26: If yes, which technologies do these policies include? (check all that apply)

#	Answer		Response	%
1	Use of computers, laptops, and tablets issued by the organization		89	91%
2	Use of cell phones issued by the organization		73	74%
3	Use of personal cell phones, laptops and other technologies		60	61%
4	Use of social media for organizational purposes		73	74%
5	Use of personal social media in reference to working for the organization		52	53%
6	Use of public WiFi		21	21%
7	Protection of passwords		65	66%
8	Accessing files and sensitive electronic documents		66	67%
9	Protection of backups, disks, tapes, software, manual		54	55%
10	Other		2	2%
11	Do Not Know		5	5%

Other
use of password manager (Dashlane) is a practice, not a policy
Record Retention and Destruction Policy

Statistic	Value
Min Value	1
Max Value	11
Total Responses	98

Q27: Who is responsible for information security for the organization? (check all that apply)

#	Answer		Response	%
1	Executive Director		81	56%
2	Manager / Director		66	46%
3	Staff Member		49	34%
4	Consultant		24	17%
5	Volunteer		7	5%
6	Third-Party Vendor		25	17%
7	Other		9	6%
8	Do Not Know		10	7%

Other
Director of Finance
IS when it comes to my computer/printer/fax/office phone
University
everyone
Our computer technician
County, City
County IT Office
no one, explicitly
The City's IT department.

Statistic	Value
Min Value	1
Max Value	8
Total Responses	144

Q28: Who in your organization is responsible for the legal requirements for information security? (e.g. GLBA, HIPPA compliance, protective orders, etc.) (check all that apply)

#	Answer		Response	%
1	Executive Director		89	62%
2	Manager / Director		61	42%
3	Staff Member		30	21%
4	Consultant		5	3%
5	Volunteer		0	0%
6	Third-Party Vendor		5	3%
7	Other		12	8%
8	Do Not Know		22	15%

Other
Chief Program Officer and Director of Finance
ED in conjunction with board attorney
Larger org has a COO and a compliance committee tasked with ensuring compliance (but just beginning its work)
board members and pro bono attorneys
Board of Directors
We are exempt from HIPPA compliance. We have internal policies based on our ethical responsibilities
University
All staff
Legal Counsel
County District Attorney
in consultation with agency counsel
Clinical Director

Statistic	Value
Min Value	1
Max Value	8
Total Responses	144

Q29: Are the legal requirements listed in Question 28 regarding information security understood by those responsible?

#	Answer		Response	%
1	No		10	7%
2	Yes		82	57%
3	Do Not Know		52	36%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.29
Variance	0.35
Standard Deviation	0.59
Total Responses	144

Q30: Has your organization identified areas or practices that may be attractive targets or vulnerable for a cyber attack or breach?

#	Answer		Response	%
1	No		41	28%
2	Yes		43	30%
3	Not yet, but will soon		8	6%
4	Do Not Know		52	36%
	Total		144	100%

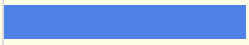
Statistic	Value
Min Value	1
Max Value	4
Mean	2.49
Variance	1.55
Standard Deviation	1.25
Total Responses	144

Q31: Has your organization experienced a cybersecurity attack or breach?

#	Answer		Response	%
1	No		87	60%
2	Yes, within the past 2 years.		10	7%
3	Yes, within the past 10 years.		4	3%
4	Do Not Know		43	30%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	2.02
Variance	1.84
Standard Deviation	1.36
Total Responses	144

Q32: Does your organization consider itself prepared to handle a cybersecurity breach or attack?

#	Answer		Response	%
1	No		42	29%
2	Yes		29	20%
3	Do Not Know		73	51%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.22
Variance	0.76
Standard Deviation	0.87
Total Responses	144

Q33: Has your organization conducted information security workshops or training with

staff, volunteers, and other stakeholders?

#	Answer		Response	%
1	No		71	49%
2	Yes		48	33%
3	Plan to Soon		4	3%
4	Do Not Know		21	15%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	4
Mean	1.83
Variance	1.08
Standard Deviation	1.04
Total Responses	144

Q34: If yes or plan to soon, who will conduct the training? (check all that apply)

#	Answer		Response	%
1	Executive Director		15	18%
2	Manager / Director		16	19%
3	Staff Member		18	21%
4	Consultant		13	15%
5	Volunteer		2	2%
6	Third-Party Vendor		16	19%
7	Other		6	7%
8	Do Not know		31	37%

Other
Web based training we take every year
Security officer
NNEDV
n/a
until recently we had IT Manager
Someone trained by NNEDV

Statistic	Value
Min Value	1
Max Value	8
Total Responses	84

Q35: Does your organization document who has access to sensitive files, databases, and

other electronic information?

#	Answer		Response	%
1	No		25	17%
2	Yes		97	67%
3	Do Not Know		22	15%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.98
Variance	0.33
Standard Deviation	0.57
Total Responses	144

Q36: Does your organization inform or train new employees about information security policies and procedures?

#	Answer		Response	%
1	No		20	14%
2	Yes		111	77%
3	Do Not Know		13	9%
	Total		144	100%

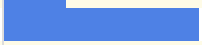
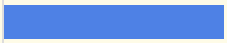
Statistic	Value
Min Value	1
Max Value	3
Mean	1.95
Variance	0.23
Standard Deviation	0.48
Total Responses	144

Q37: Does your organization inform third-party vendors, partners, and external stakeholders about your information security policies and procedures?

#	Answer		Response	%
1	No		36	25%
2	Yes		62	43%
3	Do Not Know		46	32%
	Total		144	100%

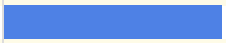
Statistic	Value
Min Value	1
Max Value	3
Mean	2.07
Variance	0.57
Standard Deviation	0.75
Total Responses	144

Q38: If your organization does use third-party vendors do they inform you of their information security policies and procedures?

#	Answer		Response	%
1	No		17	13%
2	Yes		53	41%
3	Do Not Know		60	46%
	Total		130	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.33
Variance	0.49
Standard Deviation	0.70
Total Responses	130

Q39: How is access to electronic files containing sensitive information stored within your organization protected? (check all that apply)

#	Answer		Response	%
1	Dedicated hardware (e.g. dedicated computer)		60	42%
2	Secure passwords		107	74%
3	Encryption software (e.g. Trucrypt)		25	17%
4	Smartcard		2	1%
5	Third-party storage (e.g. cloud storage)		28	19%
6	Biometrics (e.g. finger-print reader)		0	0%
7	Other		8	6%
8	Do Not Know		31	22%

Other
In our victims services program, we have one computer no connected to the internet; this is the only place PII is entered and is used to provide a number to each person served (that is not derived from PII)
Non-electronic
security policy in AD
dedicated password protected not connected to internet
drobo units so we don't ever have to use the cloud
Secure database
Firewalls

Statistic	Value
Min Value	1
Max Value	8
Total Responses	144

Q40: Does your organization have policies and procedures for the destruction of electronic documents?

#	Answer		Response	%
1	No		48	33%
2	Yes		54	38%
3	Do Not Know		42	29%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	1.96
Variance	0.63
Standard Deviation	0.79
Total Responses	144

Q41: Does your organization have policies and procedures for the destruction of storage devices? (e.g. DVDs, CDs, thumbdrives, etc.)

#	Answer		Response	%
1	No		47	33%
2	Yes		50	35%
3	Do Not Know		47	33%
	Total		144	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.00
Variance	0.66
Standard Deviation	0.81
Total Responses	144

Q42: Does your organization have access to external resources and experts to help with information security?

#	Answer		Response	%
1	No		23	16%
2	Yes		91	64%
3	Do Not Know		29	20%
	Total		143	100%

Statistic	Value
Min Value	1
Max Value	3
Mean	2.04
Variance	0.36
Standard Deviation	0.60
Total Responses	143

Q43: Please provide any additional information regarding the current state of information

security within your organization.

Text Response
personally identifiable or confidential client info is not stored on computers hard drives but is stored in the cloud - we use Box with 2-step verification that requires a code texted to the Director for access to client files
Needs improvement
We do not put any sensitive information on our computers or electronic devices due to not being able to afford appropriate electronic security.
I keep most on paper, some on my computer
Multi use agency not just dv/sa and its complex when its multifaceted agency providing child care, fitness club etc.
These questions are helpful for my own personal awareness; I need to seek more information in these areas. Thank you!
Use secure client database that meets HUD standards for security
We could be more secure.
You are scaring us!
It is a top priority and our funders are pushing our limits
We do not keep most sensitive information electronically.
paperwork-security shredding
We believe that we try to stay on top of information security but improvements could be made. medium
We recently switched from internal IT manager to third party consultant (vendor) -- not sure if it will work
We have no budget for these issues. If any professional assistance has been offered, it has been done ad hoc or by volunteers.
Our computers are so old, nobody seems to want to crash in
We have a policy that prohibits use of email to "transmit information identifying...[program] participants, his/her children or the abusive partner."
Information regarding clients and case management is done verbally. There are no client files on any computer.

Statistic	Value
Total Responses	19

Q44: If you would like to receive a statistical summary of this survey at the conclusion of this study, please provide your contact information.

Statistic	Value
Total Responses	51

Q45: Timing

#	Answer	Average Value	Standard Deviation
1	First Click	12.61	54.40
2	Last Click	227.08	304.62
3	Page Submit	236.79	306.11
4	Click Count	27.88	15.76

VITA

VITA

Kelley K. Misata

Education

- Doctor of Philosophy, August 2016, Purdue University
- Master of Business Administration, May 1995, Bentley University
- Bachelor of Science in Business Administration, May 1990, Westfield University

Professional Experience

- President / Executive Director (2013 - Present), Open Information Security Foundation
- Adjunct Faculty (2015 - Present), Emerson College
- Founder (2010 - 2013), Light the Dark
- Director of Outreach and Communications (2012 - 2014), The Tor Project, Inc.
- Business Strategist and Project Manager (2012), Independent Consultant
- Director of Research (2010 - 2012), The Institute for Applied Network Security
- Director of Strategic Initiatives (2008 - 2010), Watermark Retirement Communities
- Project Manager / Marketing (2006 - 2008), Yahoo! Inc.
- Consultant (1997 - 2006), Misata International
- Consultant / Fundraising and Program Founder (2001 - 2006), Marin Day Schools
- Consultant / Fundraising and Education (2003 - 2005), California Academy of Sciences
- Process Improvement Manager (1996 - 1997), Centric Corporation
- Learning Consultant (1995 - 1996), Columbia Sportswear
- Quality Manager / Facilitator (1994 - 1995), Scudder, Stevens and Clark
- Software Trainer (1993 - 1994), Catapult Software Training

- Project Manager (1990 - 1993), First Data Corporation, A Division of American Express

Publications

- Digital Security Breaches: Arming Crisis Organizations with New Insights, 2016 ITERA Conference Katherine B. Snow Award Winner
- The Intersection Between Privacy and Risk Communication and InfoSec: Kelley Misata Interview Part I, IBM Security
- Reframing What We Think We Know About Privacy and Risk: Part II of the Kelley Misata Interview, IBM Security
- Teaching Millennials About Privacy and Risk Communications: Part III of the Kelley Misata Interview, IBM Security
- Information Security, Privacy, and the Law in Crisis Organizations, ISSA_Journal_August_2015
- A Taxonomy of Privacy – Protecting Tools to Browse the World Wide Web, 2014 ITERA Conference

Speaking Engagements

- 21st (2016) Annual Advocacy in Action Conference
- RSA 2016
- MozFest 2015
- ISSA New England Chapter Meeting 2015
- GR3YNOISE Interview at DefCon
- National Network to End Domestic Violence Tech Summit (NNEDV) 2014 & 2015
- LASCON 2014 & 2015
- Women in Cyber Security Conference 2014 & 2015
- Investigative Reporters and Editors Conference
- Online News Association Conference
- South by Southwest 2013 & 2014
- Dartmouth College
- Purdue University Center for Education and Research in Information Assurance and Security

- McDevitt Cyber Security Lecture Series
- Massachusetts Assistant District Attorney Association
- Bentley University
- REACH Beyond Domestic Violence
- Lasell College
- Sudbury-Wayland-Lincoln Domestic Violence Roundtable
- Brookline District Schools
- Lincoln Technical Institute
- B-casa (Brookline Coalition Against Substance Abuse)
- Boston Security Meet-Up